#3

Attorney's Docket No.: 442-010085-US(PAR)

PATENT 02-07-01

0360

03645

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:. HAVERINEN et al.
Serial No.: 09/756,346
Filed: 1/8/01
For: AUTHENTICATION IN A PACKET DATA NETWORK

Group No.:

Examiner:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country	**: Finland**
Application Number	**: 20000760**
Filing Date	**: 31 March 2000**

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 CFR 1.4(f) (emphasis added.)

SIGNATURE OF ATTORNEY
Clarence A. Green

Reg. No.: 24,622

Type or print name of attorney

Tel. No.: (203) 259-1800

Perman & Green, LLP

Customer No.: 2512

P.O. Address

425 Post Road, Fairfield, CT 06430

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8a)

I hereby certify that this correspondence is, on the date shown below, being:

☑ MAILING

deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231

Date: 2/12/01

☐ FACSIMILE

transmitted by facsimile to the Patent and Trademark Office

Deborah J. Clark
Signature

DEBORAH J. CLARK
(type or print name of person certifying)

(Transmittal of Certified Copy [5-4]

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 9.1.2001

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Corporation** **Helsinki**
Patenttihakemus nro Patent application no	**20000760**
Tekemispäivä Filing date	**31.03.2000**
Kansainvälinen luokka International class	**H04L**

Keksinnön nimitys
Title of invention

"Authentication in a packet data network"
(Autentikointi pakettidataverkossa)

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Authentication in a packet data network – autentikointi pakettidataverkossa – autentikering i ett paketdatanät

This invention relates to mobile packet networks and is particularly, but not necessarily, related to authentication of a mobile node connecting to a mobile IP (Internet Protocol) network.

In mobile IP networking, a terminal, such as a laptop computer having a Wireless Local Area Network (WLAN) adapter coupled thereto, connects to its home agent via a foreign agent. In functional terms, the terminal acts as a mobile node in the network. The terms mobile node, home agent and foreign agent are explained in publication RFC2002 as follows:

Mobile Node (MN): A host or router that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming that link-layer connectivity to a point of attachment is available.

Home Agent (HA): A router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.

Foreign Agent (FA): A router on a network being visited by the mobile node which provides routing services to the mobile node whilst it is registered. The foreign agent detunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

In the publication RFC2002, it is further explained that a mobile node is given a long-term IP address in its home network. This home address is administered in the same way as a "permanent" IP address which is provided to a stationary host. When away from its home network, a "care-of address" is associated with the mobile node and reflects the mobile node's current point of attachment. The mobile node may use its home address as the source address of IP datagrams

that it sends.

It is often desirable for a mobile node to be authenticated on connection to an IP network. One way for an IP network to recognise a mobile node using the network is by using a shared secret key known by both the network and the mobile node. The shared secret known by the network can be stored in a mobile node, but for this operation, the mobile node should be supplied to the management of the IP network. Besides, in the future, there may be many different IP networks and a mobile node should be supplied with a database of secret keys in order to have one for each of the different IP networks with which it could be connected. Therefore, both entities, that is the mobile node and the IP network, must have a shared secret to be used as the cryptographic key. However, in the interest of security, the shared secret should not be provided over a network which is susceptible to eavesdropping.

Now an authentication method, devices and system has been invented for authenticating a packet data network user. A shared secret of a telecommunications network and its subscriber is used for providing shared secret for a packet data network into which the mobile node attempts to connect.

According to a first aspect of the invention there is provided an authentication method for authenticating a mobile node to a packet data network, comprising the steps of:

providing a mobile node with a mobile node identifier and a shared secret specific for the mobile node identifier;

sending a mobile node identifier to the packet data network;

sending a challenge from the packet data network to the mobile node;

generating in the mobile node a first response responsive to the challenge, based on the shared secret;

sending the first response to the packet data network; and

verifying the first response for detecting whether the use of the mobile node is authorised;

characterised by the method further comprising the steps of:

sending the mobile node identifier from the packet data network to a telecommunications network having the shared secret;

receiving the challenge from the telecommunications network and providing it to the packet data network.

Preferably, the challenge is sent from the telecommunications network to the mobile node via the packet data network.

Preferably, said method further comprises the steps of:

providing a communications link between the packet data network and the mobile node for communicating said challenge between the packet data network and the mobile node;

whereby said communications link is not a link of the telecommunications network.

Preferably, the method further comprises the step of using a Subscriber Identificating Module for the providing the mobile node with the mobile node identifier and the shared secret specific for the mobile node identifier.

Preferably, the method further comprises the steps of receiving a second response code from the telecommunications network and verifying the first response code by comparing the first response code with the second response code. Alternatively, the method comprises the steps of generating in the telecommunications network a second response code and comparing in the telecommunications network the first response code with the second response code.

Preferably, the method further comprises the steps of:

generating a protection code;

computing a cryptographic checksum using at least the protection code, the challenge, and the shared secret; and

checking the validity of the challenge using the cryptographic checksum.

Preferably, the protection code is based on time.

Preferably, the challenge comprises n RAND codes of n GSM triplets, where n is at least one. Preferably, the challenge further comprises a hash function of the n RAND codes. Preferably, the method further comprises the step of providing the packet data network with a session key code comprising n session keys Kc corresponding to n RAND codes of the challenge. Preferably, the method further comprises the step of generating an authentication key based on the shared secret, the protection code, and on an algorithm known by the mobile node and by the packet data network. In this way, it is possible to authenticate communications between the mobile node and the packet data network. The higher the number of session keys Kc is used the stronger an authentication key K becomes.

Preferably, the packet data network is an IP network. Most preferably, the packet data network is a mobile IP network.

In an alternative embodiment, the method further comprises the step of generating for Internet Key Exchange a session key based on at least the shared secret and the challenge.

In an alternative embodiment, the step of providing the mobile node with the mobile node identifier and the shared secret specific for the mobile node identifier further comprises the steps of:

forming a local connection between the mobile node and a mobile station, whereby the mobile station has a mobile node identifier and the shared secret specific for the mobile node identifier; and

retrieving the mobile node identifier and the shared secret from the mobile station to the mobile node.

According to a second aspect, a gateway is provided for interfacing the packet data network with the telecommunications network, the gateway comprising:

means for receiving a mobile node identifier from the packet data network and means for sending it to an authentication server of the telecommunications network, which server has access to a shared secret relating to the mobile node

identifier;

means for receiving a challenge from the authentication server;

means for sending the challenge to the packet data network;

means for receiving from the mobile node a first response responsive to the challenge, based on a shared secret known by the mobile node and the telecommunications network;

means for verifying the first response for detecting whether the use of the mobile node is authorised.

According to a third aspect, a mobile node is provided for use with a method according to the first aspect of the invention.

According to a fourth aspect, a system is provided for implementing the method of the first aspect of the invention.

According to a fifth aspect, a gateway is provided for a telecommunications network for implementing the method according to the first aspect of the invention.

According to a sixth aspect, a computer program is provided for implementing the method according to the first aspect of the invention.

According to a seventh aspect, a computer program product is provided for implementing the method according to the first aspect of the invention.

According to an eighth aspect, a memory medium is provided preserving a computer program of the fifth aspect of the invention.

In an alternative embodiment, the method comprises the step of authenticating the mobile node to the packet data network with a preliminary authentication method before authenticating the mobile node to the packet data network.

Advantageously, by utilising the secret shared between the telecommunications network and the mobile node, subscriber identification modules can be used for

authentication. This provides a straightforward trustworthy authentication procedure in which existing authentication data of the telecommunications network can be used.

The invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 shows a system comprising an IP network having an IP networking compliant mobile station according to a preferred embodiment of the invention;

Figure 2 shows a session key exchange procedure of a system of Figure 1;

Figure 3 shows an authentication extension according of a system of Figure 1;

Figure 4 shows the format of a new session key request extension of a system of Figure 1;

Figure 5 shows the format of a new session key reply extension of a system of Figure 1;

Figure 6 shows a SRES (signed result) extension of a system of Figure 1.

Figure 7 shows architecture of a mobile communication system according to a another embodiment of the invention;

Figure 8 shows significant functional blocks of a system of figure 7;

Figure 9 shows the major signalling events of a system of figure 7;

Figure 10 shows a detailed signalling chart of an authentication operation of a system of figure 7;

Figure 11 shows the functionality of a public access controller (PAC) during the authentication of a system of figure 7;

Figure 12 shows the functionality of the GSM/ General Packet Radio Service GPRS Authentication and billing Gateway (GAGW) during the authentication of a system of figure 7;

Figure 13 shows the major signalling of a controlled disconnection of the mobile terminal from the network of a system of figure 7;

Figure 14 shows an Internet Key Exchange procedure when the terminal is an initiator of Internet Key Exchange negotiation according to yet another embodiment of the invention; and

Figure 15 shows modifications to the procedure of Figure 14 when the PAC instead of the terminal is an initiator of Internet Key Exchange negotiation.

In the following, a preferred embodiment of the invention will be described applied to a GSM telecommunications network. As will be seen, the invention makes use of a SIM card which additionally is used for authenticating GSM subscribers according to the GSM standard. A packet data network terminal, or mobile node, can be authenticated with the SIM card. For authenticating the mobile node to a packet data network, the SIM and the GSM telecommunications network communicate across the packet data network rather than the GSM telecommunications network. Hence, the actual type of the telecommunications network is irrelevant. For example, the invention applies to a GSM/GPRS (General Packet Radio Service) network as well as to a native GSM telecommunications network. This is natural since GPRS can be understood to be an extension to GSM rather than an independent network in the sense that GPRS operates using GSM radio access network and GSM authentication methods.

The invention will be described using three examples. Example 1 relates to a mobile IP implementation, where existing mobile IP extensions are utilised. Example 2 relates to a wireless LAN environment with roaming from one subnet to another.
Example 3 relates to generation of IKE keys for Internet nodes.

EXAMPLE 1 : MOBILE IP

In the preferred embodiment of the invention, mobile nodes are identified by an International Mobile Subscriber Identifier (IMSI) in the form of a string of digits. In mobile IP messages, the IMSI is transmitted as a Network Access Identifier (NAI). The NAI may be in form of imsi@sonera.fi (e.g. "1234567@sonera.fi") or imsi@gsm.org (e.g. "1234567@gsm.org"). The IMSI can be in a different form as well. For example, in the GSM, the IMSI is represented by bytes fewer than the number of digits in the IMSI. The latter of those two examples of NAI, the gsm.org

domain, is an example on an upper level domain that is adapted to seek for the appropriate domain relating to the relevant GSM telecommunications network operator. Identifying mobile nodes with NAIs is known to a person ordinarily skilled in mobile IP. An NAI extension can be included in a Registration Request or a Registration Reply, both of which are described later.

Figure 1 shows a system comprising an IP network having an IP networking compliant mobile station according to a preferred embodiment of the invention. The mobile node is typically a laptop computer with a wireless network adapter and software for networking. A plurality of mobile nodes MN can be attached to the network. The mobile IP network is connected to a mobile telecommunications network MNW by a GSM Authentication Gateway GAGW. The GAGW couples together a server in the GSM telecommunications network and a server in the mobile IP network. These servers are designated as a home AAA server HAAA (AAA refers to Authentication, Authorisation and Accounting) and as a foreign AAA server FAAA. HAAA is located in the GSM telecommunications network and FAAA is located in the mobile IP network. Communication between the two AAA servers is here referred to as an AAA protocol. The AAA protocol is not described here. The mobile station is equipped with a GSM SIM card 111.

Operation of the SIM card 111 in the GSM telecommunications network will now be explained. In GSM, there are known authentication algorithms which are referred to as A3 and A8. These algorithms run on the SIM and in the GSM telecommunications network. These algorithms and a shared secret K_i are known by the SIM and the GSM telecommunications network operator, which typically stores them in an HLR (Home Location Register).

In authentication, the GSM telecommunications network operator generates a 128 bit random code RAND, which is to be used as a challenge, and corresponding 64 bit session key Kc and 32 bit response SRES for verifying the response to the challenge. The 64 bit session key Kc is generated by the A8 algorithm as $A8(K_i,RAND)$ and the 32 bit long SRES results from $A3(K_i,RAND)$. The combination RAND, SRES and Kc is generally referred to as a GSM triplet. The

GSM telecommunications network operator transmits the challenge RAND, the SIM receives it and reproduces SRES and Kc. Then the SIM responds to the operator with the SRES. The operator receives the SRES and can confirm the identity of the SIM. Simultaneously, the GSM telecommunications network operator can verify that it shares a common session key Kc with the SIM. Then GSM session key Kc can then be used to encrypt data traffic over the radio channel. The advantage of this challenge – response mechanism is that Kc never need be sent over air interface and thus it cannot be eavesdropped.

The authentication method according to the preferred embodiment is now briefly be described. In order to authenticate a mobile node for a packet data network, a session key K is generated both in the mobile node and in the FAAA server. Authentication is carried out using a telecommunications network (e.g., a GSM telecommunications network) and its Subscriber Identifying Module SIM. In this case the authenitcation procedure will be similar to that described above in relation to a basic GSM network. Authentication utilises the shared secret K_i which is present on the SIM and in the telecommunications network. The SIM is accessed by providing a mobile node (e.g. a laptop computer with a wireless local area network adapter) with a SIM card slot or SIM card reader. Alternatively, the packet data network does not directly access the shared secret of the telecommunications network, but receives a challenge relating to the SIM. This challenge is sent to the mobile node and the response to the challenge is verified against the correct answer that the telecommunications network can produce. Authentication can be further improved by using multiple challenges in order to generate an authentication key which is more secure than just Kc of the GSM triplet.

Figure 2 shows a session key exchange procedure of a system of Figure 1. In the following, the procedure is briefly summarised and then described in more detail.

1. The mobile node MN sends to the FAAA a Network Access Identifier NAI and a protection code MN_RAND (also known in Mobile IP terminology as nonce) generated by the mobile node. The protection code remains the same during an authentication session and it is meant to prevent replay attacks. The

protection code is typically a random number or based on time (a timestamp with certain resolution).

2. The FAAA sends to the HAAA an initial identification message containing the IMSI or NAI of the MN, and the protection code MN_RAND.
3. The HAAA retrieves n GSM triplets, each comprising a challenge RAND, a GSM session key Kc, and a response SRES. Then, the HAAA computes a session key K = H (n*Kc,MN_RAND) for the mobile node. Here n is an integer greater than or equal to 1, * represents the number of parameters (n*Kc refers to n different Kcs) and H () represents a one-way hash function. The HAAA also computes a value SIGNrand which is calculated from MAC(K,n*RAND,MN_RAND), where MAC denotes a message authentication code. SIGNrand is a cryptographic checksum dedicated to verify that the n RANDs really originate from an entity that has access to the GSM shared secret K_i (as K is derived from that). The checksum also indicates if the RANDs indeed are generated during the same authentication session because the MN_RAND changes from one authentication session to another.
4. The HAAA sends n RANDs, the SIGNrand and optionally the IMSI to the FAAA. The IMSI itself need not be used if another session identifier has been sent with the IMSI in step 1 of this procedure. In this case, this session identifier would be used instead of the IMSI.
5. The FAAA sends at least one RAND and SIGNrand to the mobile node.
6. Using the GSM shared secret K_i stored on the SIM, the mobile node calculates the session key K. Using the session key K, the n RANDs and the MN_RAND, the mobile node then tests SIGNrand. If SIGNrand matches, the mobile node generates a copies of the n SRESs (one for each RAND). The mobile node computes for the session key K and the SRESs a cryptographic checksum SIGNsres = HASH2(K,n*SRES).
7. The mobile node sends the SIGNsres to the FAAA. In the mobile node, the calculation of the session key K is similar to its calculation in the HAAA.
8. The FAAA sends the SIGNsres to the HAAA.
9. The HAAA verifies that SIGNsres is valid by checking that the equation SIGNsres = HASH2(K,n*SRES) applies with the values the MN has received.

The HAAA sends the result (whether the SIGNsres is valid) to the FAAA. If the SIGNsres is valid, the HAAA sends also the session key K to the FAAA.

10. Authentication is complete and the FAAA and the terminal share the session key K.

The FAAA is functionally connected to several HAAAs and the FAAA selects the correct HAAA based on the domain part of the user's NAI, for example "sonera.fi". The HAAA uses a HAAA-HAAA protocol to send the initial identification message to the right HAAA or GSM infrastructure (MSC, Mobile Switching Centre). According to an alternative embodiment, the FAAA knows just one HAAA and always sends the message in step 1 to that HAAA.

The session key K exchange procedure described above will now be described in more detail. The first message is a Registration Request that contains a New Session Key Request extension. This and the following extensions are explained later, referring to Figures 3 to 6. The IMSI can be transmitted in the NAI extension. The New Session Key Request extension contains a maximum key lifetime and a random number MN_RAND picked by the mobile node. When the mobility agent receives the Registration Request with the New Session Key Request extension, it sends the NAI (containing the IMSI) and MN_RAND to the HAAA. If the mobility agent is a home agent operated by a GSM telecommunications network operator, the home agent may have direct access to GSM triplets. In an embodiment of the invention, a some triplets are retrieved in advance in order to speed up the registration. Once the HAAA has obtained n GSM triplets for the mobile node by whatever means, it calculates the new session key K and an authenticator SIGNrand, as described above.

The mobility agent then sends a Registration Reply with a New Session Key Reply extension to the mobile node. This message contains the MN_RAND and the SIGNrand, so that the mobile node is able to verify that the RANDs are current and that they were generated by the GSM infrastructure. This message also contains the remaining key lifetime, which can be equal to, or smaller than, the key lifetime proposed by the mobile node.

If the mobile node and the mobility agent do not share a security context, the authentication of the first Registration Request and the Registration Reply will fail. The reply code in the Registration Reply is "mobile node failed authentication" or "identification mismatch". In the mobile IP, an authentication extension is used. The authentication extension has a special value for a security parameter index (SPI) field, meaning "New Session Key Exchange". The SPI and the IP address of the mobile node are used as an index for managing authentication procedures regarding different mobile nodes. The authentication extension has also a field for an authenticator, that is typically a MAC code. The authenticator can be empty. Thus, if the mobility agent does not support authentication according to the present invention, it will simply reply with the reply code "Mobile node failed authentication". If the mobility agent is a foreign agent, the mobile node should omit the authentication extension altogether.

After receiving the Registration Reply with the New Session Key Reply extension, the mobile node is able to verify the validity of SIGNrand. If SIGNrand is valid, the mobile node generates the key K and SIGNsres and creates a new security context for the agent or, if such already exists, updates the context with the new session key K. This key will used as the Mobile IP authentication key in subsequent registration messages.

The mobile node includes SIGNsres in a SRES extension in the next registration request it sends to the mobility agent. The mobility agent sends SIGNsres to the HAAA, which verifies it and sends an indication to the mobility agent. If SIGNsres is valid, the HAAA also sends the session key K to the mobility agent. Now the mobility agent can create/update the security context for the mobile node.

If the mobility agent is a foreign agent, the session key K could now be distributed to all the foreign agents in the visited domain.

Since the mobility agent may need to get the SRES extension quickly, in the preferred embodiment, the mobile node sends the Registration Request with the SRES extension immediately after reception of the RAND.

The security context created by the session key exchange mechanism described above has a SPI. Here, another well-known SPI is used for the SIM-generated security context. A value is reserved for the SPI "SIM-generated security context" and for the SPI "new session key exchange".

According to the preferred embodiment, the default algorithm in Mobile IP authentication is keyed MD5 in prefix+suffix mode. In this mode, an authentication digest for a message is calculated by running MD5 over the following stream of bytes: a first occurrence of the shared secret and the protected fields from the registration message and a second occurrence the shared secret.

The authentication digest is transmitted in an authentication extension as shown in Figure 3. Figure 3 shows an exemplary bit map as a table of bits, wherein each row has 3 bit octets and continues from the left hand side of the next row beneath the previous row. There are three kinds of authentication extensions: a mandatory Mobile-Home authentication extension used between the mobile node and the home agent, an optional Mobile-Foreign authentication extension used between the mobile node and the foreign agent, and an optional Foreign-Home authentication extension used between the foreign agent and the home agent. All these extensions have the same format. SPI is an opaque identifier. The verifier (that verifies the recipient of the message) of the authentication extension maps the SPI and the peer's IP address to a security context in the mobility security association database. The security context contains a key, the algorithm and other security parameters. The authenticator field contains the message digest.

In Mobile IP authentication according to the preferred embodiment, the security contexts (including the shared secret) are generated by using the SIM. Because the RAND is generated by the GSM telecommunications network, for example by the HAAA, the mobile node first sends its IMSI to the mobility agent with which it is

registering. Then the mobility agent is able to use the FAAA-HAAA protocol in order to obtain GSM authentication information for the mobile node (as described above) and use this information for generating a shared secret, i.e. the session key K, with the mobile node. After the shared session key K has been generated, the mobile node is able to register with/through the mobility agent. The session key K can be used for several subsequent registrations. However, there is a lifetime for this session key and before the lifetime expires, a new session key can be generated by a similar procedure.

The session key exchange messages between the node and the mobility agent are transmitted as extensions to the Registration Request and Registration Reply. Three new extensions to registration messages between the mobile node and the mobility agent are needed in order to agree upon the session key. These extensions are a New Session Key Request extension, a New Session Key Reply extension and a SRES extension.

Typically, the mobile node knows that its home agent supports the authentication according to the present invention. However, the mobile node may not know which authentication method or methods the foreign agent supports. To test whether the foreign agent supports the authentication method according to the invention, the mobile node includes the New Session Key Request extension for the foreign agent in the first Registration Reply and omits the Mobile-Foreign authentication extension. The New Session Key Request extension is optional. If the foreign agent does not support it, the foreign agent should ignore it and remove it before forwarding the request to the home agent. When the mobile node receives the Registration Reply, it implements the following logic:

- If the Registration Reply contains a New Session Key Reply extension and the reply code from the foreign agent is the error code "mobile node failed authentication", the foreign agent supports authentication according to the present invention. If the New Session Key Reply is valid, the mobile node creates a security context for the foreign agent and includes an SRES extension for the foreign agent in the next Registration Request.

- If the foreign agent did not set the reply code to an error code and the Registration Reply does not contain a New Session Key Reply extension and the reply code from the foreign agent is not set, the foreign agent does not support the authentication but alternatively allows registrations without Mobile-Foreign Agent authentication. The mobile node can carry out subsequent registrations with the foreign agent without any authentication extensions being required.
- If the Registration Reply does not contain a New Session Key Reply extension and the reply code from the foreign agent is the error code "mobile node failed authentication", the foreign agent does not support invented authentication and so does require different kind of authentication. In this case, a terminal with only the authentication functionality according to the present invention cannot register with the foreign agent.

When a foreign agent according to the invention receives a Registration Request from a mobile node with which the foreign agent does not share a security context, the foreign agent has the following options:
- If there is an invalid Mobile-Foreign Agent authentication extension in the Registration Request, the foreign agent replies with the error code "mobile node failed authentication". This is the standard Mobile IP behaviour.
- If the Registration Request does not contain a Mobile-Foreign authentication extension and if the local policy does not require Mobile-Foreign authentication, the foreign agent forwards the Registration Request to the home agent. The foreign agent does not include a New Session Key Reply extension in the Registration Reply even if there was a New Session Key Request extension in the Registration Request. This is the standard Mobile IP behaviour. This configuration could be useful, for example, in corporate access zones.
- If the local policy in the foreign agent requires Mobile-Foreign authentication, and there is no Mobile-Foreign Authentication extension nor New Session Key Request extension in the Registration Request, the foreign agent replies with the error code "mobile node failed authentication". This is the standard Mobile IP behaviour.
- If the local policy in the foreign agent requires Mobile-Foreign authentication, and the Registration Request contains a New Session Key Request extension and no

Mobile-Foreign Authentication extension, then the foreign agent does not forward the Registration Request to the home agent but instead replies with the error code "mobile node failed authentication" and includes a New Session Key Reply extension in the Registration Reply. If the mobile node then sends another Registration Request with a valid SRES extension and a valid Mobile-Foreign Authentication extension, the foreign agent forwards the request to the home agent.

Only certain GSM subscribers are authorised to register through a particular mobility agent. User authorisation may be done in any of the following entities:
- the GSM infrastructure. The GSM telecommunications network operator network (MSC/HLR) may support authentication according to the present invention for certain subscribers only.
- the HAAA. The HAAA may be configured with a list of authorised IMSIs. The HAAA may have a separate list for each access controller with which it is connected. This allows the HAAA to decide which subscribers are authorised users of a certain mobility agent. If the home agent is operated by the GSM telecommunications network operator, the HAAA may conveniently store this kind of authorisation information.
- the FAAA. If a corporation operates the FAAA, for example for its employees, the corporation might want to control which GSM subscribers are allowed to register with the FAAA. In this case, the mobility agent needs to maintain a list of authorised GSM subscribers. The mobility agent also needs to see the IMSI in cleartext. If public key cryptography is used between the MS and HAAA to protect the IMSI, the HAAA may need to send the cleartext IMSI to the mobility agent so that the agent can check whether the mobile node is authorised to register to the FAAA.

The new session key exchange extensions are normal (non-critical) extensions, preferably stored in an MN-AAA authentication extension. Alternatively, the session vendor-specific extensions can be used. If the receiver of a registration message does not recognise the extension, the extension is skipped.

Session key exchange between the mobile node and the foreign agent is independent of the session key exchange between the mobile node and the home agent. Thus, according to the preferred embodiment, a Registration Request contains any one of the following:

- A New Session Key Request extension for the foreign agent,
- a New Session Key Request extension for the home agent,
- a New Session Key Request extension for both the foreign agent and the home agent,
- an SRES extensions for the foreign agent,
- an SRES extension for the home agent,
- an SRES extension for both the foreign agent and the home agent,
- a New Session Key Request extension for the foreign agent and an SRES extension for the home agent, or
- an SRES extension for the foreign agent and a New Session Key Request for the home agent.

According to the preferred embodiment, a Registration Reply contains any one of the following:

- a New Session Key Reply extension from the foreign agent,
- a New Session Key Reply extension from the home agent, or
- a New Session Key Reply extension from both the foreign agent and the home agent.

The format of the New Session Key Request Extension is shown in Figure 4. The mobile node may place the New Session Key Request Extension with a sub-type 1 (MN-FA) after the Mobile-Home authentication extension and before the Mobile-Foreign authentication extension (if present). The foreign agent must remove this extension from the request before forwarding the request to the home agent.

The mobile node may place the New Session Key Request extension with a sub-type 2 (MN-HA) before the Mobile-Home authentication extension.

As can be seen from Figure 4, the format of the New Session Key Request Extension is as follows:

Type	Value 134 (skippable)
Length	The length of this extension in bytes, not including the Type and Length fields. For the New Session Key Request extension, the length is 26 bytes.
Reserved	Reserved for future use. The value is 0.
Vendor/Org-ID	The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of a vendor of a mobile networking service, in network byte order.
Vendor Type	NEW_SESSION_KEY_REQUEST_VENDOR_TYPE. This value indicates that the particular type of this extension is a New Session Key Request extension. The administration of the Vendor-Types is done by the Vendor
Subtype	1: MN-FA New Session Key Request extension 2: MN-HA New Session Key Request extension
Key Lifetime	Maximum key lifetime in seconds, two bytes long.
MN_RAND	A random number generated by the mobile node (16 bytes or 8 bytes).

This is an example on use of a vendor specific extension. Alternatively, another type of mobile IP specified extension can be used.

The format of the New Session Key Reply Extension is shown in Figure 5. The foreign agent may insert the New Session Key Reply extension with sub-type 1 (MN-FA) in a Registration Reply after the Mobile-Home authentication extension (if present) and before the Mobile-Foreign authentication extension (if present). The home agent may insert the New Session Key Reply with sub-type 2 (MN-HA) in a Registration Reply before the Mobile-Home authentication extension.

As can be seen from Figure 5, the format of the New Session Key Reply Extension is as follows:

Type	Value 134 (skippable)
Length	The length of this extension in bytes, not including the Type and Length fields. For the New Session Key Reply extension, the length is 42 bits + the length of n RANDs.
Reserved	Reserved for future use. To be set to 0.
Vendor/Org-ID	Value e.g. 94 (Nokia). The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of vendor in network byte order.
Vendor-Type	This value indicates that the particular type of this extension is a New Session Key Reply extension. The administration of the Vendor-Types is done by the Vendor.
Subtype	1: FA-MN New Session Key Reply extension 2: HA-MN New Session Key Reply extension
Key Lifetime	Remaining key lifetime in seconds
SIGNrand	The authenticator for n RANDs, 16 bytes.
n*RAND	n GSM RANDs (length n·16 bytes).

The format of the SRESR extension is shown in Figure 6. The mobile node may place the SRES extension with sub-type 1 (MN-FA) in a Registration Request after the Mobile-Home authentication extension and before the Mobile-Foreign authentication extension (if present). The foreign agent must remove this extension before forwarding the Registration Request to the home agent.

The mobile node may place the SRES extension with sub-type 2 (MN-HA) in a Registration Request before the Mobile-Home authentication extension.

As can be seen from Figure 4, the format of the SRES extension is as follows:

Type	134 (skippable)
Length	The length of this extension in bytes, not including the Type and Length fields. For the New SRES extension, the length is 23 bytes.
Reserved	Reserved for future use. To be set to 0.
Vendor/Org-ID	The high-order octet is 0 and the low-order 3 octets are the

	SMI Network Management Private Enterprise Code of vendor in network byte order, as defined in the Assigned Numbers RFC [Assigned numbers].
Vendor-Type	This value indicates that the particular type of this extension is an SRES extension. The administration of the Vendor-Types is done by the Vendor.
Subtype	1: MN-FA SRES extension 2: MN-HA SRES extension
SIGNsres	The response calculated by the mobile node, 16 bytes.

In another embodiment of the invention, the session key exchange messages between the Mobile Node and the Foreign Agent are transmitted by extending agent discovery messages to include IMSIs and RANDs.

In yet another alternative embodiment, an opaque authenticator field is used in the authentication extension. The beginning of this extension is used for sending RANDs, key lifetimes and other session key exchange parameters. The key exchange parameters are included in the calculation of the authenticator.

If the parameters are transmitted in a separate extension before the authentication extension, the data for key exchange becomes automatically included in the computation of the authentication extension. Furthermore, using separate extensions makes the system easier to implement. The authenticator is the result of the MAC function, e.g. a SIGNrand as computed according to step 2.

In a further embodiment, instead of using well-known SPIs for the SIM-generated security contexts, SPIs are communicated in the new session key exchange messages.

A GSM/GPRS SIM based user mobility management functionality (user authentication and billing) can be used for public WLAN access zone authentication and billing functions. The SIM based authentication involves relatively trustworthy verifying the user's identity (authentication) for charging the

user. The GSM core GSMCORE provides roaming services for a GSM mobile station roaming between various operator networks. Advantageously, the roaming service is implemented using existing SIM cards and the GSM infrastructure. Consequently, the WISP roaming should not require any extra security keys from the MT. Furthermore, all the GSM users who obtained WLAN roaming service from their home operator have requisite the MT, SIM and necessary roaming software to be able to access the public network. A home operator provides the roaming MT with a SIM card for authenticating with it. GSM2 is alternatively a GSM telecommunications network supporting GPRS.

EXAMPLE 2 : A WIRELESS LAN

Figure 7 shows an architecture of a mobile communication system according to another embodiment of the invention. The system comprises a terminal MT, two public Wireless IP access networks WISP1 and WISP2, the Internet INET, a first GSM telecommunications network GSM1 and a second GSM telecommunications network GSM2 connected to a GSM core GSMCORE. The public wireless IP access network (WISP1,WISP2) offers wireless broadband IP services for so that the terminals can roam in public hot spots, such as hot spots provided by hotels, airports etc. The WISP network can be operated either by a GSM telecommunications network operator or by a private ISP with a roaming agreement with a GSM telecommunications network operator. The roaming agreement is essential for SIM authentication. The terminal can connect to a WISP. The terminal can also roam from one network to another using a known technique. In Wireless Local Area Network, the roaming from one WLAN hot spot to another is referred to as WLAN roaming service. The WISPs have access to the Internet INET.

The terminal MT has an equipment part ME and a SIM provided for use with the second GSM telecommunications network GSM2. The MT may not be a GSM compliant mobile station. In this case a user of the MT can access the second GSM telecommunications network GSM2 by providing a GSM mobile station with a SIM. In a preferred embodiment, the MT is a laptop computer equipped with a WLAN adapter card (not shown) and a smart card reader (not shown) that can use

the SIM. Alternatively, the MT is a device having a GSM mobile station part for communicating with GSM telecommunications networks and a WLAN terminal part for communicating with WLANs.

Both GSM telecommunications networks GSM1 and GSM2 comprise respective Mobile Switching Centres MSC1 and MSC2. The GSM core couples these MSCs together. Furthermore, the first GSM telecommunications network has a GSM/GPRS Authentication and Billing GateWay (GAGW) coupling it to the Internet INET. The GAGW is the GSM telecommunications network operator's entity which provides the GSM authentication services to WISPs and collects the charging information.

GSM telecommunications networks which are connected to the GSM core can further be connected through it and through the GAGW to the WISP (to which the MT is connected) and to the mobile MT for authentication and billing purpose as will be described in more detail later.

The operation of the system will now be described. The user has a GSM agreement with GSM telecommunications network operator B (of GSM2) and so it is the user's home network operator. The network operator B has signed a roaming agreement with GSM telecommunications network operator A (of GSM 1). The GSM telecommunications network operator A has partner arrangements with the operators of WISP1 and WISP2, referred to, respectively, as operators C and D. The roaming user with the SIM may roam from WISP1 to WISP2. Both WISPs send authentication request messages to the network operator A. The GSM core network roaming functionality is used for relaying the authentication messages to the subscriber's home operator B (GSM2). The architecture allows users of either GSM telecommunications network to roam with their MTs between WISPs, although the WISPs have direct connection only to operator A network GSM1.

A roaming user need not have a pre-established customer relationship with a WISP. Instead, the roaming user may rely on his customer relationship with his home GSM telecommunications network in order to provide authentication and

billing in the WLAN. WISP access is charged to the roaming user's GSM bill via a GSM telecommunications network operators' authentication gateway.

Here, these roaming services are used for allowing an mt to be authenticated and charged using GSM SIM both for accessing the GSM core as well as public IP access networks. The GSM telecommunications network operator bills the user for both the authenticating/roaming services and for the use of public IP access networks. Then, the GSM telecommunications network operator reimburses the use of public IP access networks for their operators.

In an alternative embodiment of the invention, the GSM telecommunications network operator may provide the subscriber with a WISP roaming SIM, which does not allow use of the GSM radio services. Such a dedicated SIM can be used to authenticate and debit services provided by a WLAN.

As is known from the GSM, the home GSM network stores customer information, such as authentication codes and user identity. Typically, this information is stored in a GSM Home Location Register (HLR). The GSM telecommunications network operator provides the IP based authentication and charging interface for one or several WISP operators, possibly also or only for corporate access solutions.

The GAGW supports seamless roaming between various GSM telecommunications network operators. The WISP sends all the authentication and billing information to the GAGW. The GAGW uses GSM core signaling known from GSM and conveys the authentication and billing information to the corresponding home GSM telecommunications network operator. The signalling of billing information between different GSM telecommunications networks can be arranged in a similar manner as when ordinarily roaming to a foreign GSM telecommunications network for a mobile telephone call. In this case, the foreign GSM telecommunications network charges the home GSM telecommunications network for its service on arranging the telephone call.

The home operator stores the charging records and sends the bill to the user. The WISP generates a billing record describing the billed services. The billing can be based on any of the known principles or combination of them, for example on flat rate, usage time or packet number or access bandwidth. The GSM network (GAGW) transmits the WISP originated records to the existing GSM billing system.

The MT supports authentication using SIM card. In an alternative embodiment, the MT supports one or more other authentication mechanisms, for example smart card authentication for corporate network access. Such a terminal contains authentication software and the SIM card but need not have keys for public access or any other security association.

Figure 8 shows significant functional blocks of a system of figure 7. Figure 8 only shows single WISP although it is understood that more than one WISP and GSM telecommunications network may be present. Figure 8 shows three important functional elements of the system: the mobile terminal MT, a Public Access Controller PAC and the GPRS/GSM Authentication and Billing Gateway GAGW. The GAGW is a dedicated entity of the GSM telecommunications network that interfaces the GSM/GPRS network with an IP network (for example, the Internet or a wide area IP network). The GAGW also offers the necessary WLAN-cellular roaming functions, in particular those related to authentication and billing services.

The PAC is the WISP's network entity which controls access from the radio access network to the Internet services. In the preferred embodiment, it allocates an IP address for the MT and authenticates the MT before the connection to the Internet is established. The PAC relays the authentication messages between the MT and the GAGW, collects the billing record and sends it to GAGW. The PAC also relays the user data traffic between the MT and the Internet.

In a preferred embodiment, the SIM authentication is a complementary service for the PAC and the PAC supports additionally other authentication mechanisms such as password based authentication.

The interfaces of the system will now be described.

The MT – PAC interface is an IP based interface that is provided with authentication functionality. The authentication is designed so that it can be embedded in a well-known standard IP protocol or implemented as an extension for the existing protocol. The MT and PAC are identified using their IP addresses in this interface.

The PAC – GAGW interface is an IP based interface that uses a suitable authentication protocol. Typically, a single GAGW supports several PACs simultaneously. The GAGW identifies various PACs with their IP addresses. In this interface, the MT identification is based on an IMSI code stored on the SIM.

The GAGW – HLR interface is implementation and vendor specific. The GAGW hides the cellular infrastructure from PACs. Therefore, the PAC-GAGW interface is always the same although the underlying cellular network may be of a different type (GSM, GPRS) or provided by a different vendor.

Figure 9 shows the major signalling steps of a system of figure 7. The process of authenticating a WLAN terminal to the PAC is typically triggered when an MT attempts to connect to the public access network. In this case, the MT acquires an IP address via a dynamic host configuration protocol (DHCP) server (not shown). The DHCP protocol and appropriate servers are well known in the art. The authentication has to be completed before the network beyond the PAC can be accessed. The MT triggers the authentication by roaming software. In an alternative embodiment, the authentication is automatically triggered when the MT tries to access to the network using SIM authentication and the roaming application is running.

An overview of the authentication is next explained by reference to the signals used during the authentication process:

301. The MT communicates with the PAC to connect to the radio access network (WISP) and to obtain an IP address from a DHCP server.

302. The PAC sends information of the supported authentication mechanisms, such as SIM authentication, Public Key Infrastructure (PKI) or pre-shared key.

303. The MT detects that SIM authentication is supported. The ME requests the IMSI from the SIM.

304. The SIM responds to the request by sending the IMSI to the ME.

305. The MT forms a Network Access Identifier that is the IMSI in a Network Access Identifier (NAI) format, for example 1234567@gsm.org, where 1234567 is the IMSI number and gsm.org is the domain name of the home GSM telecommunications network. The MT establishes a dynamic security association with the PAC, for example using Diffie-Hellman, and sends the NAI encrypted over the temporary secure channel. In an alternative embodiment, the NAI is sent as cleartext without encryption.

306. The PAC decrypts the NAI, and forwards it in a data packet, again encrypted, to the GAGW over the secure PAC-GAGW. The IP address of GAGW is statically configured in the PAC. A secure channel is formed between the PAC and the GAGW using secret they share.

307. The GAGW verifies that the packet came from a valid PAC, decrypts the packet, checks the NAI and sends it with an authentication request to the nearest MSC. Next, the MSC analyses the IMSI to find out the home HLR of the subscriber. Then, the MSC forwards the authentication request to the home HLR.

308. The home HLR forms a set of one or more GSM authentication triplets (RAND, SRES, Kc) and sends it to the originator MSC which forwards the information to the GAGW.

309. The GAGW forms a packet containing the RANDs and a cryptographic checksum of the RANDs, generated using at least the Kcs. The GAGW preserves the SRES for later use in a subsequent step 314.

310. The PAC decrypts the packet and relays the RANDs and the cryptographic checksum to the MT.

311. The MT inputs the RANDs to the SIM, which calculates corresponding Kc and SRES values.

312. The MT checks that the Kcs match with the cryptographic checksum given by the PAC. If they match, the MT knows that the PAC has a connection to the HLR and so the PAC can be trusted.

313. The MT generates a cryptographic checksum for the SRESs with Kc and sends the checksum to the PAC.

314. The PAC relays the checksum of the SRES to the GAGW. The GAGW checks that the checksum matches with the SRESs it received from the MSC in step 308. If it matches, the GAGW sends an acknowledge message ACK to the PAC. If it does not match, then the GAGW sends a negative acknowledge NACK to the PAC.

315. If the PAC receives a positive acknowledge message ACK confirming successful authentication, it completes the authentication by opening the access to the Internet. If the PAC receives a negative acknowledge message NACK, it refuses to open access to the Internet.

In an alternative embodiment, the IMSI is used in the preceding steps instead of the NAI.

The following tables list the information elements that are carried between elements of the system:

Table 1 Main parameters transferred between the MT and the GAGW

Parameter	Direction to	Encryption	Explanation
IMSI/NAI	GAGW	X	User ID for cellular network side
RAND	MT		Random authentication Challenge
SRES	GAGW	x	Authentication response to the HLR
Hash(K_MT)	MT	X	Authentication checksum for the MT
Hash(K_GAGW)	GAGW	X	Authentication checksum for the GAGW

Table 2 Main parameters transferred between the MT and the PAC

Parameter	Direction to	Encryption	Explanation
IMSI/NAI	PAC	X	User ID for cellular network side
Bill_ind	MT		Information of the costs

Table 3 Main parameters transferred between the PAC and the GAGW

Parameter	Direction to	Encryption	Explanation
Bill_ind	PAC		Access pricing info
User_class	PAC	x	User class/profile (business, consumer, ...)
K_RAN	PAC	x	Air interface encryption key
CDR	GAGW	x	User's billing record (structure tbd)

In the preferred embodiment, an optional user_class parameter is used for defining the quality of service, for example the maximum bandwidth for a particular user.

Figure 10 shows a detailed signalling chart of an authentication of a system of figure 7. The chart presents the following steps:

401. The MT sends an MT originated authentication starting request MT_PAC_AUTHSTART_REQ containing the NAI having the IMSI. The message typically also contains a protection code MN_RAND (known also as nonce in the context of mobile IP).

402. The PAC receives the message MT_PAC_AUTHSTART_REQ from the MT and requests for GSM triplets by sending to the GAGW a message PAC_GAGW_AUTHSTART_REQ, also containing the NAI and the MN_RAND.

403. The GAGW obtains the GSM triplets from the home GSM telecommunications network. One triplet suffices, but the GSM telecommunications network may return a plurality of triplets, in which case either some of the triplets are discarded or stored for later use, or according to the preferred embodiment, used to generate a stronger key. The home GSM telecommunications network is recognised using the NAI.

404. The GAGW generates a session key, using an encryption algorithm, of at least the GSM session key(s) Kc. In the preferred embodiment, the MN_RAND is also used in the encryption. The GAGW encrypts the GSM RAND(s) of GSM triplets, computes a cryptographic checksum, or a Message Authentication Code MAC, based on the RAND(s) and the session key, and prepares an authentication start response message GAGW_PAC_AUTHSTART_RESP. The encryption between the GAGW and the PAC is based on their own shared secret.

411. The GAGW sends to the PAC an authentication start response message GAGW_PAC_AUTHSTART_RESP containing the RANDs, the MAC, the MN_RAND, a billing information code and a billing information MAC computed for the billing information code. Typically, the authentication start response message additionally contains a field for session timeout parameter for determining the validity period of the new session key to be generated and a field for a state of the session.

412. The PAC forwards to the MT the authentication start response message GAGW_PAC_AUTHSTART_RESP as a PAC_MT_AUTHSTART_RESP message.

413. The MT tests with the SIGNrand that the parameters carried by the GAGW_PAC_AUTHSTART_RESP and by the PAC_MT_AUTHSTART_RESP indeed originate from the GSM telecommunications network.

414. The MT handles the billing information it received from the GAGW. Typically, it provides the user with an information of the price of the service requested by the user. Usually, this price is based on at least one of the following: a flat rate fee, a time based billing, number of data packets sent to or from the MT, and the Quality of Service QoS. The MT then asks the user whether the service should be obtained with the price given. The MT receives an answer from the user.

415. The MT generates a MAC of the SRESs to be used for responding to the GAGW.

416. The MT generates the shared secret Kpac_MT using at least the Kcs.

421. The MT generates and sends an MT_PAC_AUTHANSWER_REQ message to the PAC. The message contains in the state field the answer for the user

showing whether the user accepted the billing for the service, the MAC of the SRESs, a MAC of the billing code, and the MN_RAND (as all the messages sent during an authenticating session).

422. The PAC generates a PAC_GAGW_AUTHANSWER_REQ containing the data of the MT_PAC_AUTHANSWER_REQ message and additionally the NAI and the IP address of the PAC.

423. The GAGW tests the MAC of the SRESs to verify that the data sent by the MT carried by the PAC_GAGW_AUTHANSWER_REQ has not been tampered.

424. If the GAGW gets a positive answer to the test, it generates the shared secret Kpac_MT in a manner similar to that used by the MT in step 416 and the proceeds to the step 431.

431. The GAGW sends to the PAC a message GAGW_PAC_AUTHANSWER_RESP_OK. The message contains the MN_RAND and codes filter_id, Kpac_MT and SIGNresult. The filter_id is an optional code and indicates the user class of the subscriber. This can be used in defining a QoS, for example a high quality connection for well paying business users. The Kpac_MT is the shared secret. The SIGNresult is a MAC of the data in the message for ultimately verifying to the MT that the reply from the GAGW is not altered on the way to the MT.

441. The PAC responds to the GAGW by a PAC_GAGW_STARTBILLING_REQ message requesting the GAGW to start the billing. The message contains the NAI, a session ID (the MN_RAND)

442. The GAGW checks the answer from the MT for verifying that the MT has permitted the billing.

451. If the MT permitted billing, the GAGW sends to the PAC a message GAGW_PAC-STARTBILLING_RESP_OK for indicating the start of billing.

452. The PAC sends to the MT a PAC_MT_AUTHANSWER_RESP_OK message containing the SIGNresult.

453. The MT receives the PAC_MT_AUTHANSWER_RESP_OK message and checks the SIGNresult it contains. If the SIGNresult is correct, the MT can inform the user of a start of billing.

The MAC of the billing code is computed at least using the Kcs so that the PAC cannot tamper the billing code.

In the message PAC_MT_AUTHANSWER_RESP_OK, the MT is notified of the term of the authentication. The MT re-authenticates itself before the authentication term expires. If it does not re-authenticate, the connection of the MT to the PAC is released and the MT can authenticate itself again.

In the preferred embodiment, the MT receives billing information and decides how to handle it. In the preferred embodiment of the invention, the user of the MT can define a billing information handling policy. This policy can be used to define, for example, that no billing information is presented to the user in a re-authentication or normal authentication case. The handling of the billing information does not affect the protocol of messaging between the different entities (MT, PAC, GAGW, MSC and HLR).

Figure 11 shows the functionality of the PAC during the authentication. In this figure, all of the blocks relate to the PAC except those that are marked as "MT" or "GAGW". The drawing will be described by referring to each of the blocks by their reference sign.

The operation starts from block 501. An MT requests authentication from the PAC by sending an MT_PAC_AUTHSTART_REQ message containing the MN_RAND and the NAI to the PAC, thus triggering the authentication process there (block 511). The PAC maps (block 512) an IP address MT_IP for the MT. The PAC checks first whether it already has an IP address mapped for that NAI. If it has, it retrieves the mapping from a database record (block 513). Otherwise it obtains an IP address and stores it with the NAI to a database for future use.

After mapping (block 512) of the IMSI with an IP address, the PAC relays (block 514) the NAI to the GAGW (block 541) in a PAC_GAGW_AUTHSTART_REQ message. The GAGW responds (block 542) by a GAGW_PAC_AUTHSTART_RESP message containing a random number RAND

to be used as a challenge. In block 515, The PAC receives the challenge and maps a session ID code SESSION_ID to the MT_IP. Next, the PAC updates the database record (block 516) by storing the SESSION_ID with the MT_IP and the IMSI. Then, the PAC sends (block 517) the challenge RAND to the MT in a PAC_MT_AUTHSTART_RESP message. The MT receives (block 502) the message, generates and responds (block 503) with an MT_PAC_AUTHANSWER_REQ message containing a cryptographic checksum SIGN_SRES corresponding to the challenge and the challenge itself. The PAC receives the SIGN_SRES and relays (block 518) it to the GAGW which checks (block 543) whether it is correct. The GAGW returns (block 544) to the PAC a GAGW_PAC_AUTHANSWER_RESP message to inform the PAC whether the SIGN_SRES is correct. Alternatively, the GAGW may compute the correct SIGN_SRES and return it to the PAC so that the PAC itself verifies whether the MT generated SIGN_SRES is correct. In either case, the PAC verifies (block 519) the response from the GAGW and decides (block 520) next actions based on the response. If the response is positive, that is successful authentication, then the PAC proceeds to block 523 to start billing. Otherwise, the execution proceeds to block 521. There, a NACK is sent as a PAC_MT_AUTH_ANSWER_RESP_ERR to the MT to indicate an error in the authentication and the SESSION_ID is removed (block 522) from the record in which it was stored.

Next, the steps related to billing are explained. In block 523, a message PAC_GAGW_STARTBILLING_REQ is sent to the GAGW. The message informs the GAGW the possibility to apply charges to the account of the user of the MT to be added in a GSM invoice. The GAGW receives (block 547) this message and replies with a message GAGW_PAC_STARTBILLING_RESP as a confirmation. The message is verified (block 524) by the PAC, and in case of a denial instead of confirmation, the PAC returns to block 521. Otherwise, (block 526) an acknowledge message PAC_MT_AUTHSTART_RESP_OK is sent to the MT to confirm the start of possible billing and a timer is started.

In the next phase, the PAC remains idle and provides periodical billing updates. These updates are triggered by debited events, such as transmission or reception

of data packets. The PAC may combine the charges and, only after a certain period of time or after reaching of a certain triggering amount of charge, perform a billing update corresponding to the lump sum thus gathered. When billing an event, the PAC sends a PAC_GAGW_UPDATEBILLING_REQ to notify the GAGW about the billing update. The GAGW receives (block 547) this message and responds (block 548) by a receipt message GAGW_PAC_UPDATEBILLING_RESP. The PAC receives (block 528) the receipt and checks (block 529) if it is positive. If the receipt is negative, the PAC prevents (block 532) MT for transferring data packets to and from the WISP, sends a billing stop to the GAGW, and sends (block 533) an authentication request to the MT for its re-authentication. On the other hand, if the receipt is positive in block 529, the PAC checks (block 530) the timer to detect a session timeout. If a timeout is detected, the PAC continues to block (block 532) and proceeds as described above. If no timeout is detected, the PAC operation returns to block 527.

Figure 12 shows the functionality of the GSM/GPRS Authentication and billing Gateway (GAGW) during authentication in a system of figure 7. Figure 11 illustrated the functionality of the PAC and here the same procedure is considered from the GAGW's point of view. The procedure starts from block 601. The PAC sends to the GAGW the PAC_GAGW_AUTHSTART_REQ message containing the IMSI and the domain name of the MT (defined by the SIM). The GAGW checks (block 611) whether the MT is already authenticated. If yes, then an authentication validity timer (described later) is stopped (block 613) and existing user information is used (block 615). Otherwise, a temporary user ID is allocated to the MT identified by the IMSI and the subscriber's data (IMSI and corresponding user ID) is stored (block 619) in a record of a database.

Then, the MT authentication is started (block 621). The GAGW requests (block 623) the GSM triplets from the home GSM telecommunications network of the subscriber by a GAGW_MSC_DATA_REQ message sent to the closest MSC 681. The MSC responds (block 682) by an MSC_GAGW_DATA_RESP message containing one or more GSM triplets and additionally information concerning whether or not the MSC allows billing for the use of the PAC by that user. The

GAGW verifies (block 627) the response. If the user is not authorised to the billing service, or alternatively, if the reply timer expires (block 625), the GAGW sends (block 629) an authorisation error message GAGW_ PAC_AUTHSTART_RESP_ERROR to the PAC (block 602). Otherwise, the timer has not expired and the verification of the response is positive and the procedure continues from block 633. The GAGW retrieves from the database (block 635) the RAND_MT and at least one GSM triplet associated to the subscriber being authenticated. Then the GAGW calculates a SIGNrand using a hash function and the Kc and RAND of (each of) the GSM triplet(s) used. This certain number of Kcs is denoted by n*Kc. Here, the asterisk does not refer to a multiplication but to the number of different valued parameters Kc. The same applies to all the other occurrences of asterisk as well. For multiplication, a dot "·" is used instead of an asterisk. As the MSC typically provides one to four different GSM triplets in response to one request, one or more triplets can be used for authentication. By using two or more triplets instead of just one, enhanced security is obtained because the keys are longer and the recurring period, in which the same key is used again, increases. This further allows increase of the validity term of the authentication keys formed.

In block 637, the GAGW sends a challenge and it's the SIGNrand in a GAGW_PAC_AUTHSTART_RESP message to the PAC (block 603). The PAC responds with a PAC_GAGW_AUTHANSWER_REQ message to indicate if the user is willing to accept the billing. The GAGW checks (block 641) the message and if it shows that the user does not accept billing, the GAGW stores (block 643) the response for statistical purposes (block 639) and sends a GAGW_PAC_AUTHANSWER_RESP message to the PAC to acknowledge to the PAC that the authentication is to be aborted. The statistical purposes include gathering information on that how many of the users have accepted and how many have not accepted the billing. This information can be used for optimising the price for the connection in order to maximise the profits of the WISP operators and GSM telecommunications network operators.

If the message PAC_GAGW_AUTHANSWER_REQ indicates that the user is willing to accept the billing, the GAGW tests (block 645) the SIGNsres. This testing is carried out by computing the SIGNres using the hash function known by the MT and using the same input data (nonce_MT, Kc and RAND of each of the GSM triplets used). For the testing, the GAGW retrieves (block 647) the input data from the database. As a next step (block 649), the GAGW tests whether the SIGNsres was indeed correct.

If the SIGNsres was incorrect, the GAGW sends (block 653) a reject message GAGW_PAC_AUTHANSWER_RESP_ERR to the PAC (block 606).

If the SIGNsres was correct, the GAGW grants the MT access and generates (block 651) a shared secret Kpac_MT. Then, the GAGW sends (block 655) access accept by a message GAGW_PAC_AUTHANSWER_RESP_OK to the PAC (block 607). Furthermore, the GAGW generates (block 657) a PAC-specific authentication ticket and stores (block 663) it. Then the GAGW updates (block 659) the user information in the database and stores (block 665) the user data comprising the generated shared secret. Finally, the GAGW starts (block 661) the authentication validity timer (mentioned also in relation to block 613) and starts an (block 667) accounting process. The authentication validity timer is preferably implemented by storing to the database the lapsing time of the authentication. This enables use of the common hardware (clock) for a plurality of different users and easy checking of expiry of the authentication by comparison of the present to the lapsing time.

Access to the WISP by the MT is charged to the user's GSM account. When the MT is authenticated to the WISP, the PAC starts collecting billing information. The PAC maintains a database of the connection time and amount of data sent. When the MT disconnects, the PAC relays this information to GAGW. The GAGW then generates a GSM Call Detailed Record (CDR) ticket and relays it to the GSM billing system known from the GSM.

Figure 13 shows the major signalling steps of a controlled disconnection of the MT from the network. The disconnecting process starts from that that the MT selects (block 711) that it be disconnected. The MT sends (block 713) an MT_PAC_DISCONNECT_REQ message to the PAC. The PAC sends (block 721) a PAC_GAGW_STOPBILLING_REQ message requesting the GAGW to stop billing. The GAGW responds by sending (block 731) a PAC_GAGW_STOPBILLING_RESP to the PAC. Finally, the PAC sends a PAC_MT_DISCONNECT_RESP message to acknowledge the MT of a successful disconnection.

EXAMPLE 3

The functional architecture of the present invention can be implemented using several suitable protocols. However, in this example an enhanced version of, an Internet Key Exchange (IKE, RFC 2409) protocol is used in communications between the MT and the PAC. Remote Authentication Dial In User Service (RADIUS, RFC 2138, RFC 2139) protocol is used for communications between the PAC and the GAGW. It should also be noted the PAC functionality could be integrated inside an access point server if needed. However, by separating the PAC functionality from the access point, handovers are easier to implement and hence the separation is appropriate for installations comprising a plurality of access points. Figure 14 shows the main signalling between the MT, the PAC and the GAGW when the enhanced IKE protocol referred to as IKE+ is used between the MT and the PAC.

HDR is an Internet Security Association and Key Management Protocol (ISAKMP, RFC 2409) header whose exchange type defines the payload orderings. When written as HDR* it indicates payload encryption. SA is an SA negotiation payload with one or more Proposal and Transform payloads. KE is the Key Exchange payload. IDmt is the identity payload for the MT.

The IKE+ protocol will now be described in detail.

The IKE+ protocol uses IKE mechanisms with enhancements. This authentication mode is an extension to ones defined in RFC2409 and is related to the one suggested by Litvin M., Shamir R., Zegman T., in "A Hybrid Authentication Mode for IKE", draft-ietf-ipsec-isakmp-hybrid-auth-03.txt, December 1999. The protocol is designed for two-way authentication between a the MT and the PAC, and uses GSM authentication in phase 1. The exchange is not symmetric, unlike the ones in the RFC2409. Instead, both IKE negotiators must know where they execute because they communicate with different components: The MT uses its attached SIM card for the authentication related functions, whereas the PAC relies on an authentication server (GAGW) in the GSM telecommunications network, in a chain:

SIM <---> MT <----------> PAC <-------> GAGW

IKE negotiation between the MT and the PAC uses the standard ISAKMP payload syntax. Other messages do not have the same syntax, and are implementation dependent.

As this exchange is rather more complicated than the ones defined in the RFC2409, it is only defined in IKE main mode. The following parameters are used in the exchange. They are contained in standard ISAKMP payloads, as explained later.

IMSI	IMSI read from the SIM card
MN_RAND	a random number generated by the MT
RAND	a random number given by the GAGW
SIGNrand	calculated by the GAGW as HMAC(Kc*n, RAND*n|MN_RAND|billinginfo), where HMAC is the MD5 algorithm of RFC1321 applied in HMAC mode described in RFC2104 and Kc is the encryption key from the SIM card
SIGNsres	calculated by the MT and the GAGW as HMAC(Kc*n, SRES*n|IMSI|MN_RAND), where SRES is the authenticator from the SIM card
Kpac_MT	calculated by the GAGW and the MT as

HMAC(Kc*n, RAND*n||IMSI||MN_RAND)

Here, the bar "|" refers to a string concatenation, wherein two sets of digits are concatenated together, for example 1234 | 567 = 1234567.

The exchange, as shown below, is vulnerable to a man-in-the-middle attack between the MT and the PAC, because of the authentication asymmetry. However, if the exchange is used over a medium such as a wireless LAN, this kind of an active attack is difficult. The fact that the GAGW only talks to PACs it knows over secure channels further reduces the likelihood of success of such an attack.

The security of the exchange can be enhanced with a public key technique, which does not remove the threat of a man-in-the-middle attack, but protects the user's IMSI: The MT may request the GAGW's certificate from the PAC, and use the public key in it to encrypt the IMSI value sent over in the IDmt payload. The IMSI value is then known only to the MT and the GAGW, and can be also used to authenticate the PAC to the MT, as explained later.

When the ID payload is used to carry the MT's IMSI, the ID Type field in the ISAKMP generic payload header is set to ID_USER_FQDN.

The following values identify the roles the IKE peers should assume. Values are taken from the private use range defined in the RFC2409 for the Authentication Method attribute and should be used among mutually consenting parties.

Type	Value	Explanation
GSMAuthInitMT	65100	IKE negotiation initiated by the MT
GSMAuthInitPAC	65101	IKE negotiation initiated by the PAC

Figure 14 shows how the exchange works when the MT is the initiator of the IKE negotiation.

The most notable exception to normal IKE practices, where only the first two messages affect the negotiated IKE SA, the final SA lifetime will be set to the sessiontimeout value selected by the GAGW. The initial lifetime is assumed to be long enough to allow the negotiation to finish and the final value to be set.

The session key between the MT and the PAC is generated as SKEYID = prf(g^xy, CKY-I | CKY-R). The values for SKEYID_{a,d,e} are computed in the usual fashion based on SKEYID.

If the GAGW is able to recognise the IMSI, it calculates SIGNrand. For sending RAND and SIGNrand over to the MT, the PAC uses nonce (Npac) and hash payloads (HASH(1)), respectively. If there is a need to send more than one RAND in a single message, they can be concatenated in the same nonce payload, or many nonces can be sent. The receiver can easily determine the sender's choice, because the size of the GSM RAND does not change frequently. If the IMSI verification fails, the PAC indicates it to the MT by using a notify payload with notification type set to INVALID-ID-INFORMATION. Other, implementation dependent, error codes may be additionally transmitted in the notify payload.

The GAGW also delivers billing information, which the PAC forwards to the MT in a notification payload (NOTIFY). The status code for the notify payload is BILLING_INFO, and uses value 32768 from the private range. The person using the MT must be queried whether she will accept the tariff offered. If she does, or if a predefined timer expires, the exchange is continued with message seven. Otherwise the MT sends a notify message to the PAC with notification type ATTRIBUTES-NOT-SUPPORTED. The MT should use a relatively short lived timer so that the protocol machine in the PAC will not be delayed excessively.

The MT calculates SIGNsres, and sends it over in HASH(2) to the PAC, which forwards it to the GAGW for verification. If the verification succeeds, the GAGW's response message contains a session key (Kpac_MT) between the MT and the PAC for later use, and a timeout value for the MT's session with the GAGW. The timeout value chosen by the GAGW updates the one agreed upon previously in

the IKE negotiation. The PAC must, therefore, send an updated IKE SA to the MT. The PAC does not send the Kpac_MT value to the MT, but instead uses it to encrypt the body of the updated SA payload. This is shown as <SA_b>Kpac_MT. The SIGNresult value from the GAGW is packaged in HASH(3) for IKE transport. If the GAGW cannot verify the MT's identity, the PAC indicates it to the MT by using a notify payload with the notification type set to AUTHENTICATION-FAILED.

Figure 15 shows the minor modifications to the procedure of Figure 14 when the PAC is the initiator. One extra message is required for the certificate passing to work. The PAC could include the GAGW's certificate in the first message, but this way the MT can decide whether it needs the certificate. The GAGW, and unchanged parts are omitted from Figure 15.

Particular implementations and embodiments of the invention have been described. It is clear to a person ordinarily skilled in the art that the invention is not restricted to details of the embodiments presented above, but that it can be implemented in other embodiments using equivalent means without deviating from the characteristics of the invention. For example, in an embodiment, the mobile node is physically a unit separate from a mobile station that has the SIM. Then, the mobile node forms a permanent link or a temporary link to the mobile station, for example low power radio frequency link such as Bluetooth link. In this case, it is not even necessary that the telecommunications network uses any separable SIMs for authenticating. The SIM functionality may be integrated to the mobile station in an inseparable manner, for example an the K_i or its equivalent can be stored in a non-volatile memory of the mobile station. Naturally, the terminal can be integrated with the mobile station so that the authenticating functionality of the mobile station is accessible to a terminal part regardless whether the mobile station is designed to use a SIM or not. In yet another embodiment, the packet data network is a fixed packet data network, for example a LAN or a Wide Area Network. In a further embodiment, the invented authentication is used for authenticating a mobile node to a service, for example to a WWW portal or an Internet banking service. Hence, The scope of the invention is only restricted by the attached patent claims.

Abbreviations

AAA	Authentication, Authorisation and Accounting
FA	Foreign Agent
GAGW	GSM Authentication Gateway
GSM	Global System for Mobile communications
GSM triplet	RAND, Kc, and SRES
HA	Home Agent
HDR	Internet Security Association and Key Management Protocol (ISAKMP) header whose exchange type defines the payload orderings
HLR	Home Location Register (a GSM telecommunications network element)
IMSI	International Mobile Subscriber Identifier, used in GSM
IPsec	Internet Protocol Security protocol
ISAKMP	Internet Security Association and Key Management Protocol
Kc	A 64 bit long key produced by a SIM
K_i	Subscriber authentication key, used in GSM and stored on the GSM telecommunications network (for example HLR) and on the SIM
MD5	Message Digest 5
MN	Mobile Node (Mobile IP client)
MSC	Mobile Switching Center (a GSM telecommunications network element)
MT	Mobile terminal
NAI	Network Access Identifier, for example user@nokia.com or imsi@gsm.org
RAND	A 128 bit random number used as a challenge in GSM authentication
RAND_MT	A random key for protecting against replay attacks, MT generated
SIM	Subscriber Identification Module
SPI	Security Parameter Index
SRES	Signed Result, a 32 bit response in GSM authentication

Claims

1. Authentication method for authenticating a mobile node to a packet data network, comprising the steps of:

providing a mobile node with a mobile node identifier and a shared secret specific for the mobile node identifier;

sending a mobile node identifier to the packet data network;

sending a challenge from the packet data network to the mobile node;

generating in the mobile node a first response responsive to the challenge, based on the shared secret;

sending the first response to the packet data network; and

verifying the first response for detecting whether the use of the mobile node is authorised;

characterised by the method further comprising the steps of:

sending the mobile node identifier from the packet data network to a telecommunications network having the shared secret;

receiving the challenge from the telecommunications network and providing it to the packet data network.

2. Authentication method according to claim 1 further comprising the step of providing a communications link between the packet data network and the mobile node for communicating said challenge between the packet data network and the mobile node; whereby said communications link is not a link of the telecommunications network.

3. Authentication method according to claim 1 or 2 further comprising the step of using a Subscriber Identificating Module (SIM) for the providing the mobile node with a mobile node identifier and a shared secret specific for the mobile node identifier.

4. Authentication method according to any of preceding claims further comprising the steps of receiving a second response code from the telecommunications network and verifying the first response code by comparing the first response code with the second response code.

5. Authentication method according to any of claims 1 to 3 further comprising the steps of generating in the telecommunications network a second response

code and comparing in the telecommunications network the first response code with the second response code.

6. Authentication method according to any of preceding claims wherein the challenge is sent from the telecommunications network to the mobile node via the packet data network.

7. Authentication method according to any of preceding claims further comprising the steps of:

generating a protection code (MN _RAND);

computing a cryptographic checksum (MAC) using at least the protection code, the challenge, and the shared secret; and

checking the validity of the challenge using the cryptographic checksum.

8. Authentication method according to claim 5, wherein the protection code is based on time.

9. Authentication method according to any of preceding claims, wherein the challenge comprises n RAND codes of n GSM triplets, where n is at least one.

10. Authentication method according to any of claim 7, wherein the challenge further comprises a hash function of the n RAND codes.

11. Authentication method according to any of claim 7 or 8, wherein the method further comprises the step of providing the packet data network with a session key code comprising n session keys Kc corresponding to n RAND codes of the challenge.

12. Authentication method according to any of claims 7 to 9, wherein the method further comprises the step of generating an authentication key (K) based on the shared secret (K_i) , a protection code (MN_RAND), and on an algorithm (A8) known by the mobile node and by the packet data network.

13. Authentication method according to any of preceding claims, wherein the packet data network is an IP network.

14. Authentication method according to any of preceding claims, wherein the packet data network is a mobile IP network.

15. Authentication method according to any of preceding claims further comprising the step of generating for Internet Key Exchange a session key based on at least the shared secret and the challenge.

16. Authentication method according to any of preceding claims, wherein the step

of providing the terminal with the mobile node identifier and the shared secret specific for the mobile node identifier further comprises the steps of: forming a local connection between the terminal and a mobile station having the mobile node identifier and the shared secret specific for the mobile node identifier; and

retrieving the mobile node identifier and a shared secret specific for the mobile node identifier from the mobile station to the terminal.

17. Gateway for interfacing the packet data network with the telecommunications network, the gateway comprising:

means for receiving a mobile node identifier from the packet data network and means for sending it to an authentication server of the telecommunications network, which server has access to a shared secret relating to the mobile node identifier;

means for receiving a challenge from the authentication server;

means for sending the challenge to the packet data network;

means for receiving from the mobile node a first response responsive to the challenge, based on a shared secret known by the mobile node and the telecommunications network;

means for verifying the first response for detecting whether the use of the mobile node is authorised.

18. System implementing the method according to any of the preceding claims.

19. Terminal of the system according to claim 18.

20. Gateway for a telecommunications network for implementing the method according to any of claims 1 to 15.

21. Computer program for implementing the method according to any of claims 1 to 15.

22. Computer program product for implementing the method according to any of claims 1 to 15.

23. Memory medium for preserving a computer program according to claim 21.

(57) Abstract

Authentication method for authenticating a mobile node to a packet data network, comprising the steps of:

providing a mobile node with a mobile node identifier and a shared secret specific for the mobile node identifier;

sending a mobile node identifier to the packet data network;

sending a challenge from the packet data network to the mobile node;

generating in the mobile node a first response responsive to the challenge, based on the shared secret;

sending the first response to the packet data network; and

verifying the first response for detecting whether the use of the mobile node is authorised;

sending the mobile node identifier from the packet data network to a telecommunications network having the shared secret;

receiving the challenge from the telecommunications network and providing it to the packet data network.

Fig. 2.

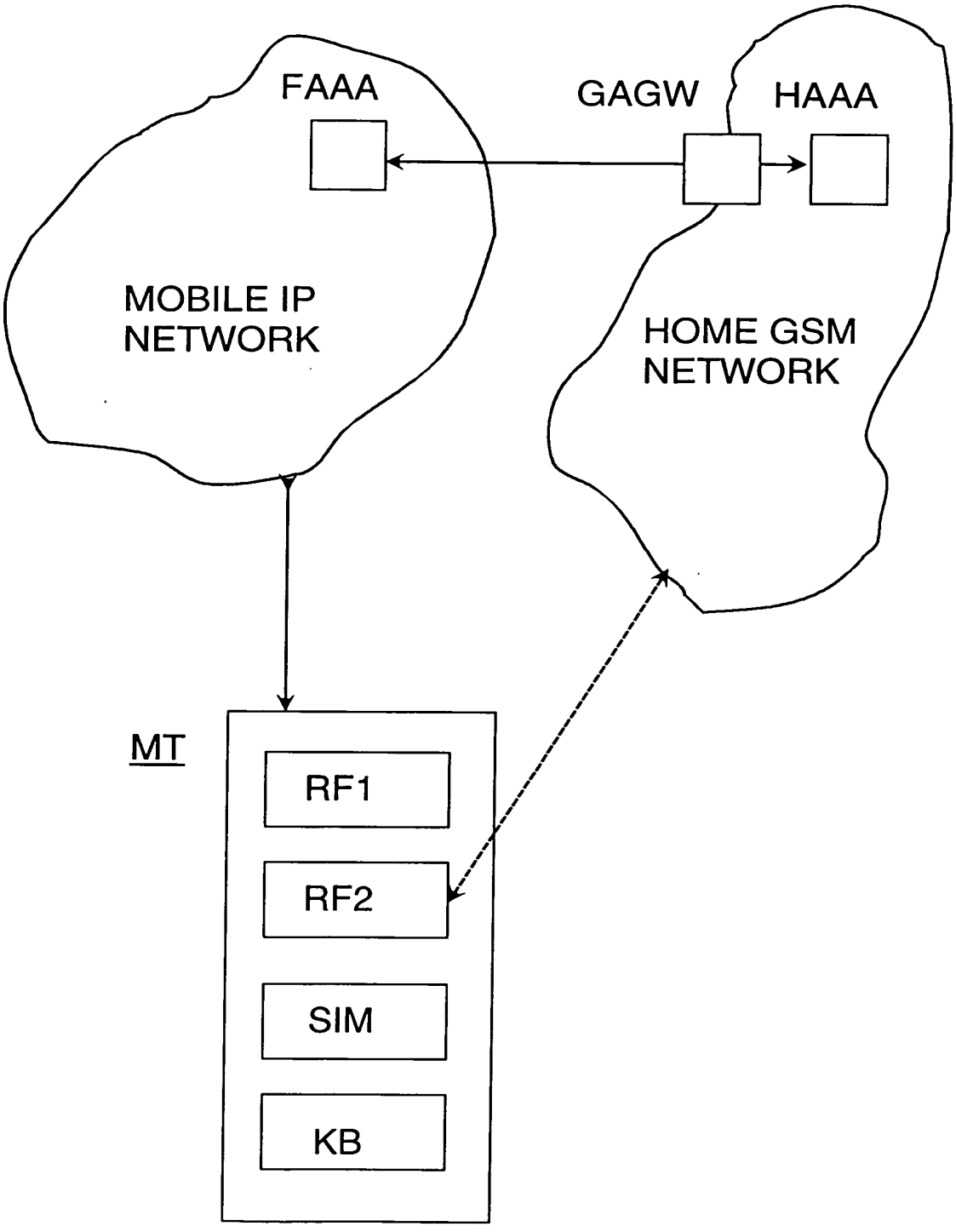
FAAA
GAGW
HAAA
MOBILE IP
NETWORK
HOME GSM
NETWORK
MT
RF1
RF2
SIM
KB

Fig. 1

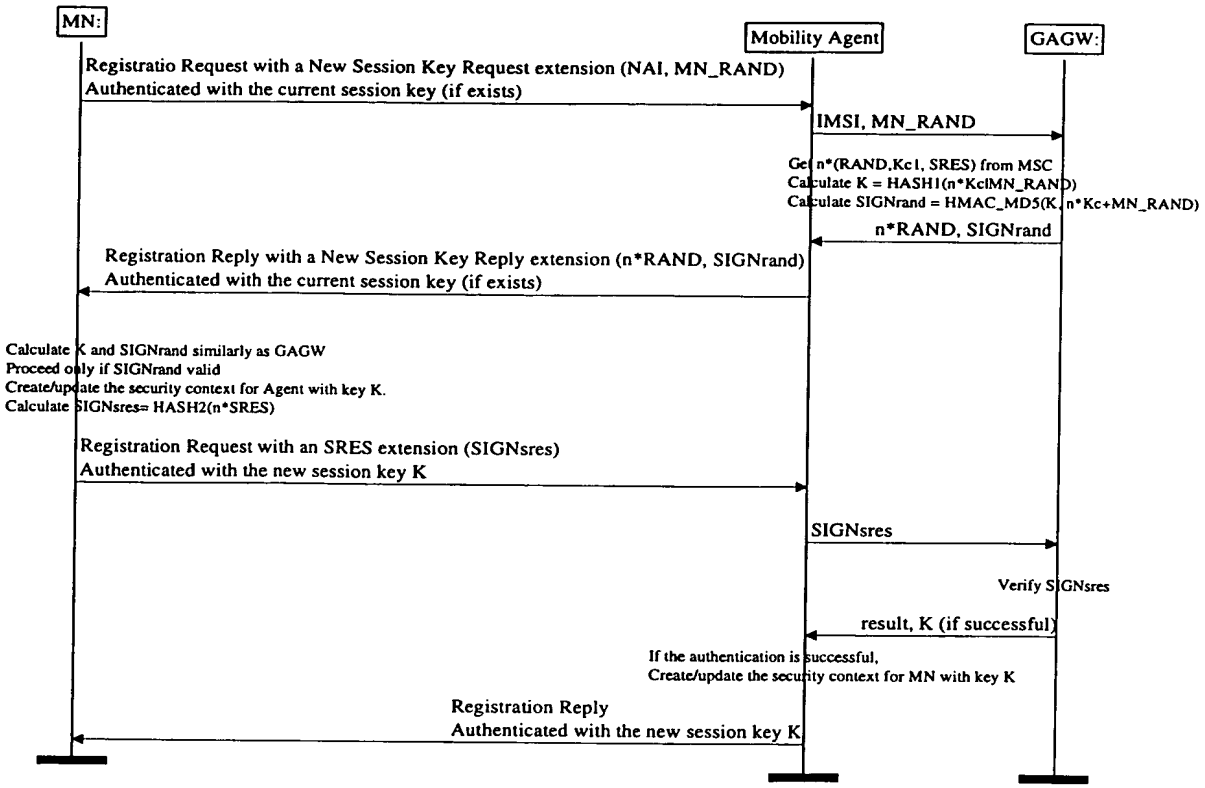

Figure 2

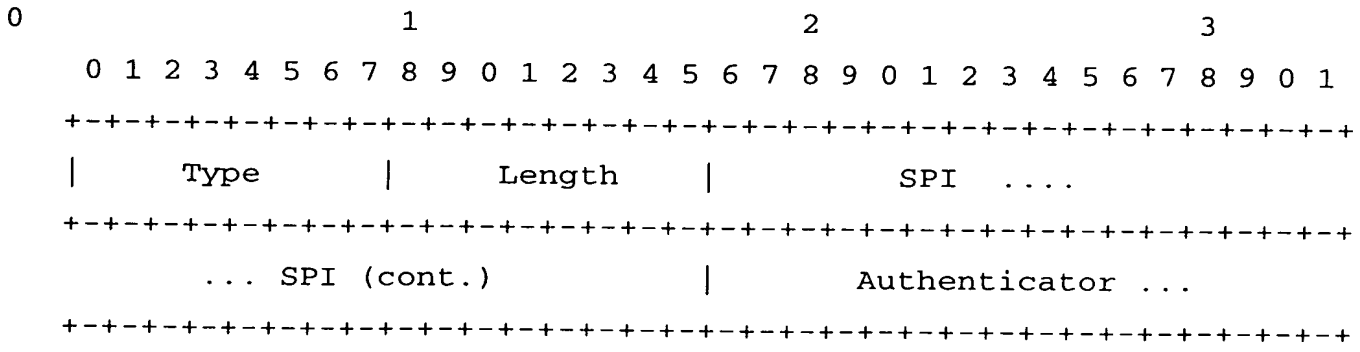

Figure 3

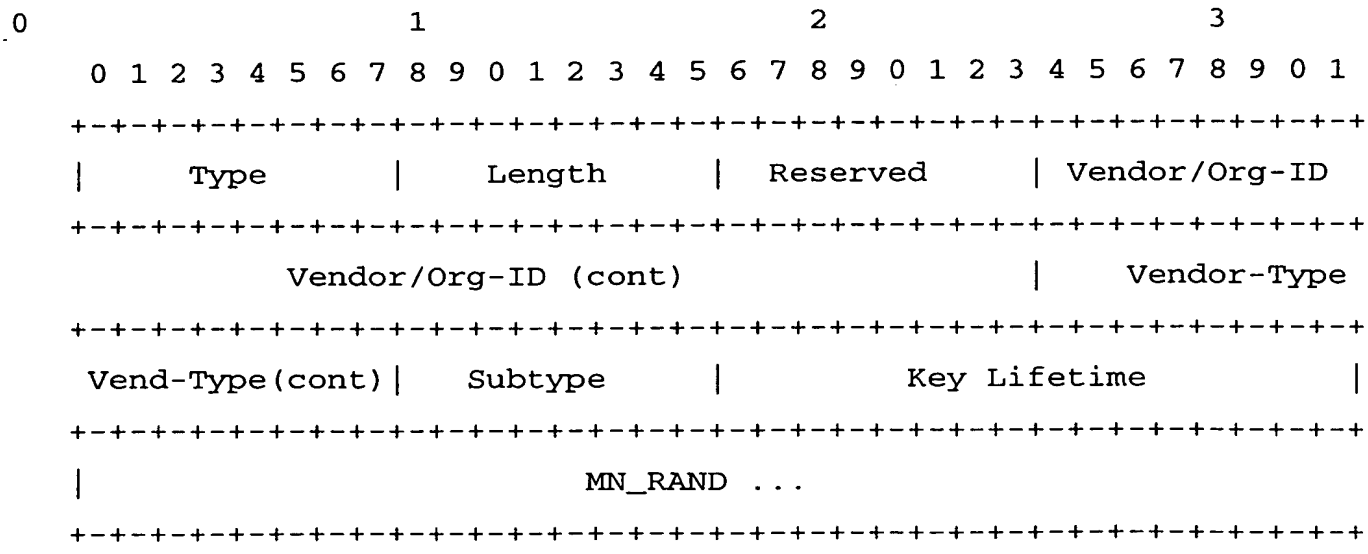

Figure 4

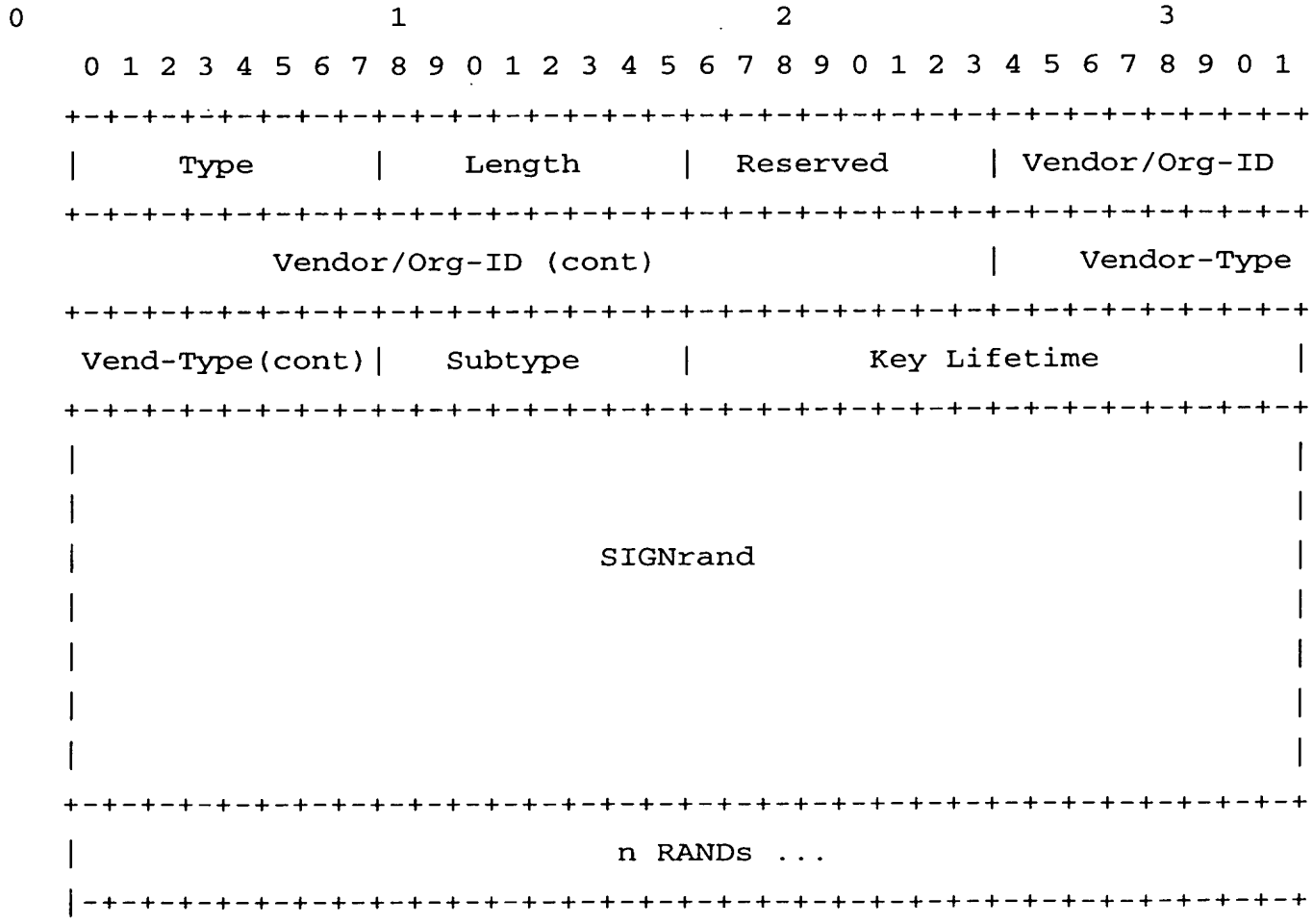

Figure 5

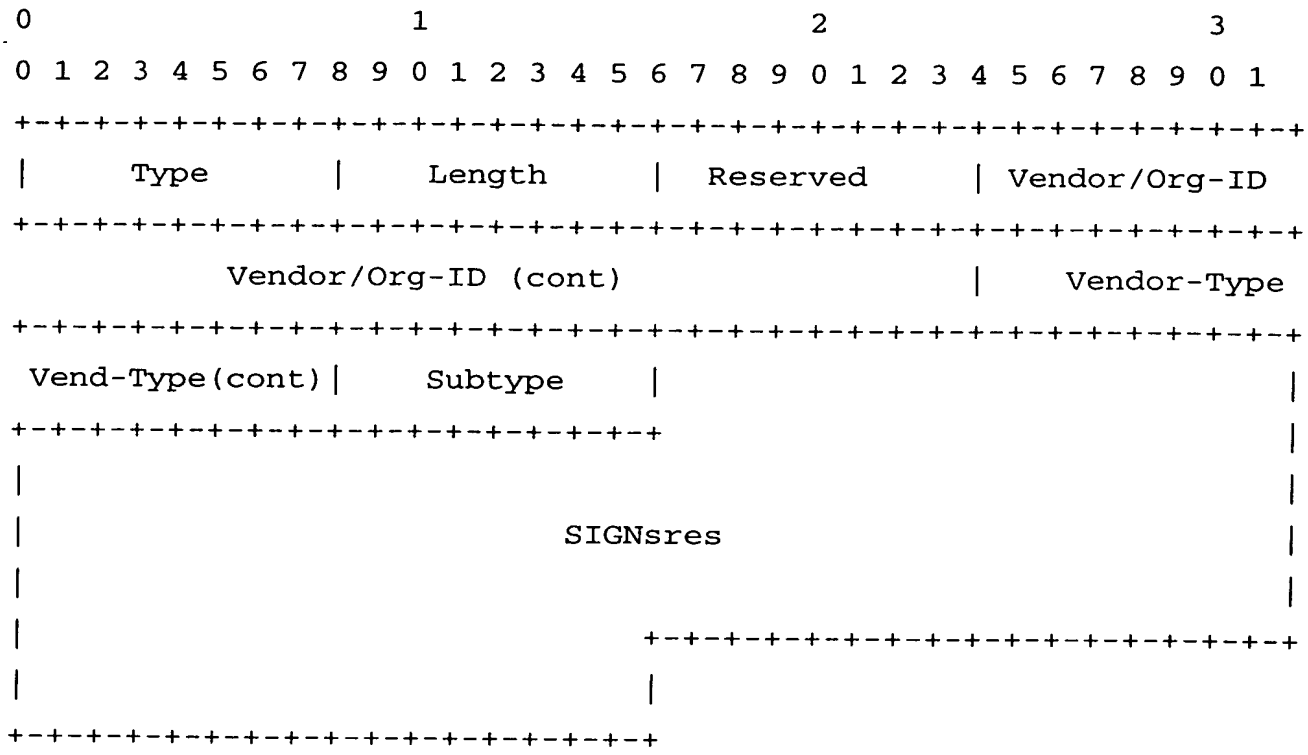
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Reserved
Vendor/Org-ID
Vendor/Org-ID (cont)
Vendor-Type
Vend-Type(cont)
Subtype
SIGNsres

Figure 6

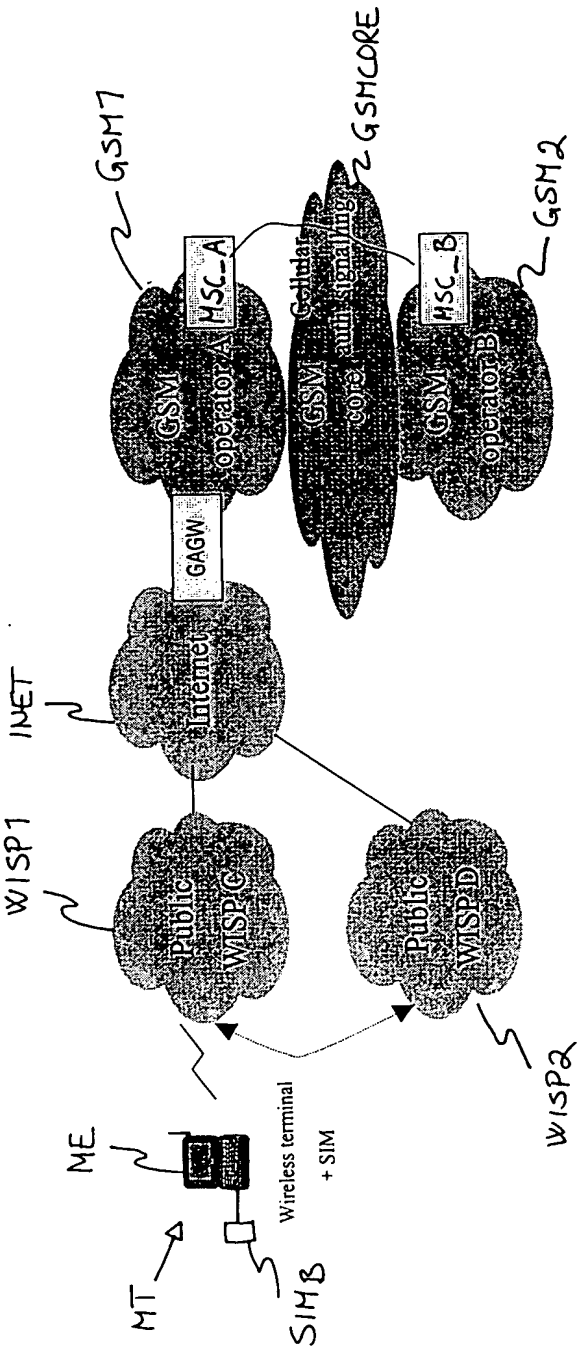
GSM1
GSMCORE
GSM2
GSM operator A
VSC_A
Cellular aum signaling
GSM core
VSC_B
GSM operator B
GAGW
Public Internet
INET
WISP1
Public WISP C
Public WISP D
WISP2
ME
Wireless terminal
+ SIM
MT
SIM
B

Fig. 7

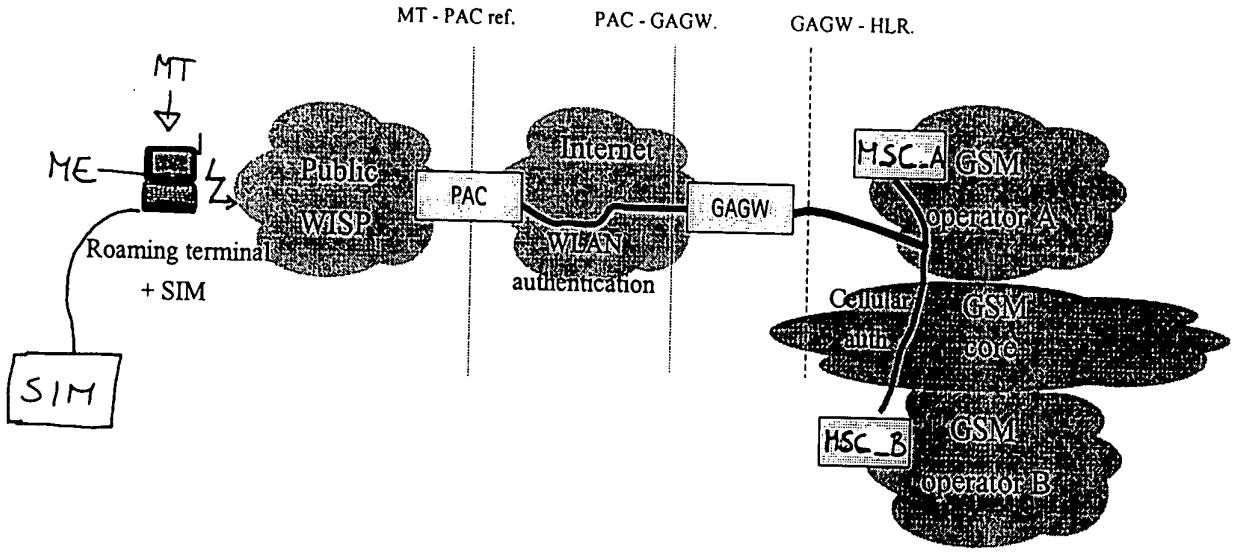
MT - PAC ref.
PAC - GAGW.
GAGW - HLR.
MT
ME
Public
WISP
PAC
Internet
WLAN
authentication
GAGW
MSC_A
GSM
operator A
Roaming terminal
+ SIM
Cellular
GSM
core
SIM
MSC_B
GSM
operator B

Fig. 8

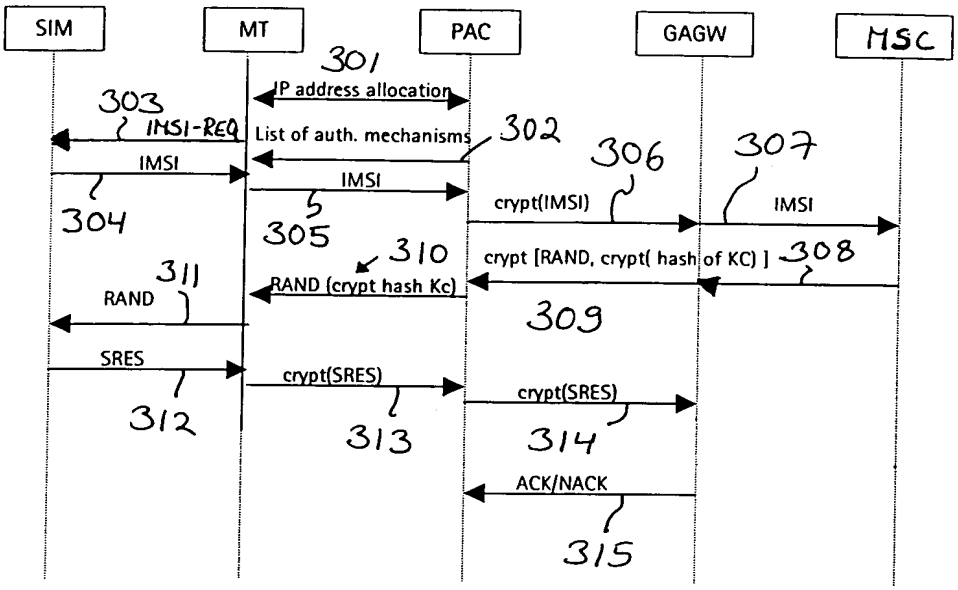
SIM
MT
PAC
GAGW
MSC
301
IP address allocation
303
IMSI-REQ
List of auth. mechanisms
302
306
307
IMSI
IMSI
crypt(IMSI)
IMSI
304
305
310
crypt [RAND, crypt(hash of KC)]
308
311
RAND
RAND (crypt hash Kc)
309
SRES
crypt(SRES)
crypt(SRES)
312
313
314
ACK/NACK
315

Fig. 9

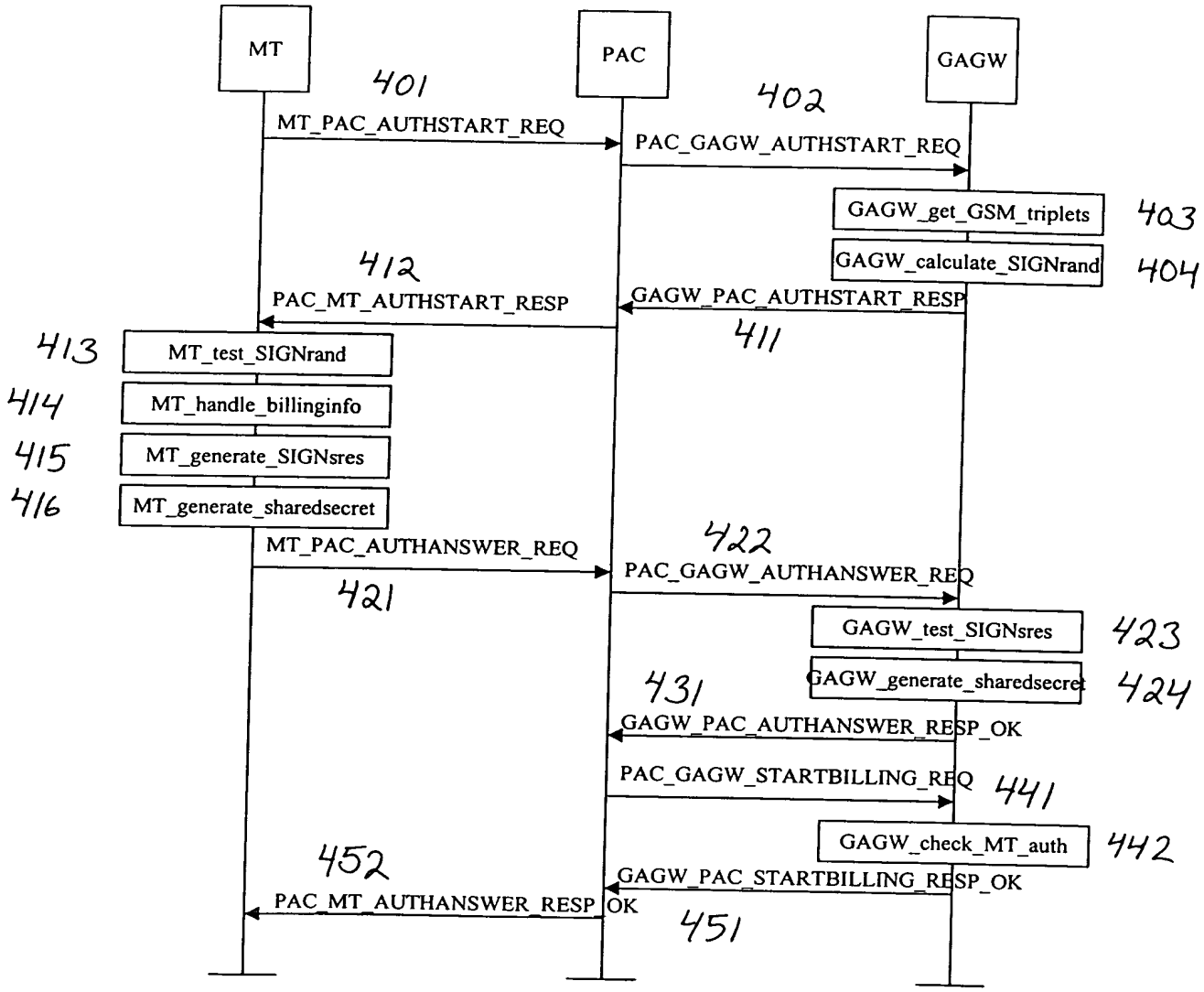
MT
PAC
GAGW
401
MT_PAC_AUTHSTART_REQ
402
PAC_GAGW_AUTHSTART_REQ
GAGW_get_GSM_triplets
403
GAGW_calculate_SIGNrand
404
412
PAC_MT_AUTHSTART_RESP
GAGW_PAC_AUTHSTART_RESP
411
413
MT_test_SIGNrand
414
MT_handle_billinginfo
415
MT_generate_SIGNsres
416
MT_generate_sharedsecret
MT_PAC_AUTHANSWER_REQ
422
PAC_GAGW_AUTHANSWER_REQ
421
GAGW_test_SIGNsres
423
GAGW_generate_sharedsecret
424
431
GAGW_PAC_AUTHANSWER_RESP_OK
PAC_GAGW_STARTBILLING_REQ
441
GAGW_check_MT_auth
442
452
GAGW_PAC_STARTBILLING_RESP_OK
PAC_MT_AUTHANSWER_RESP_OK
451

Fig. 10

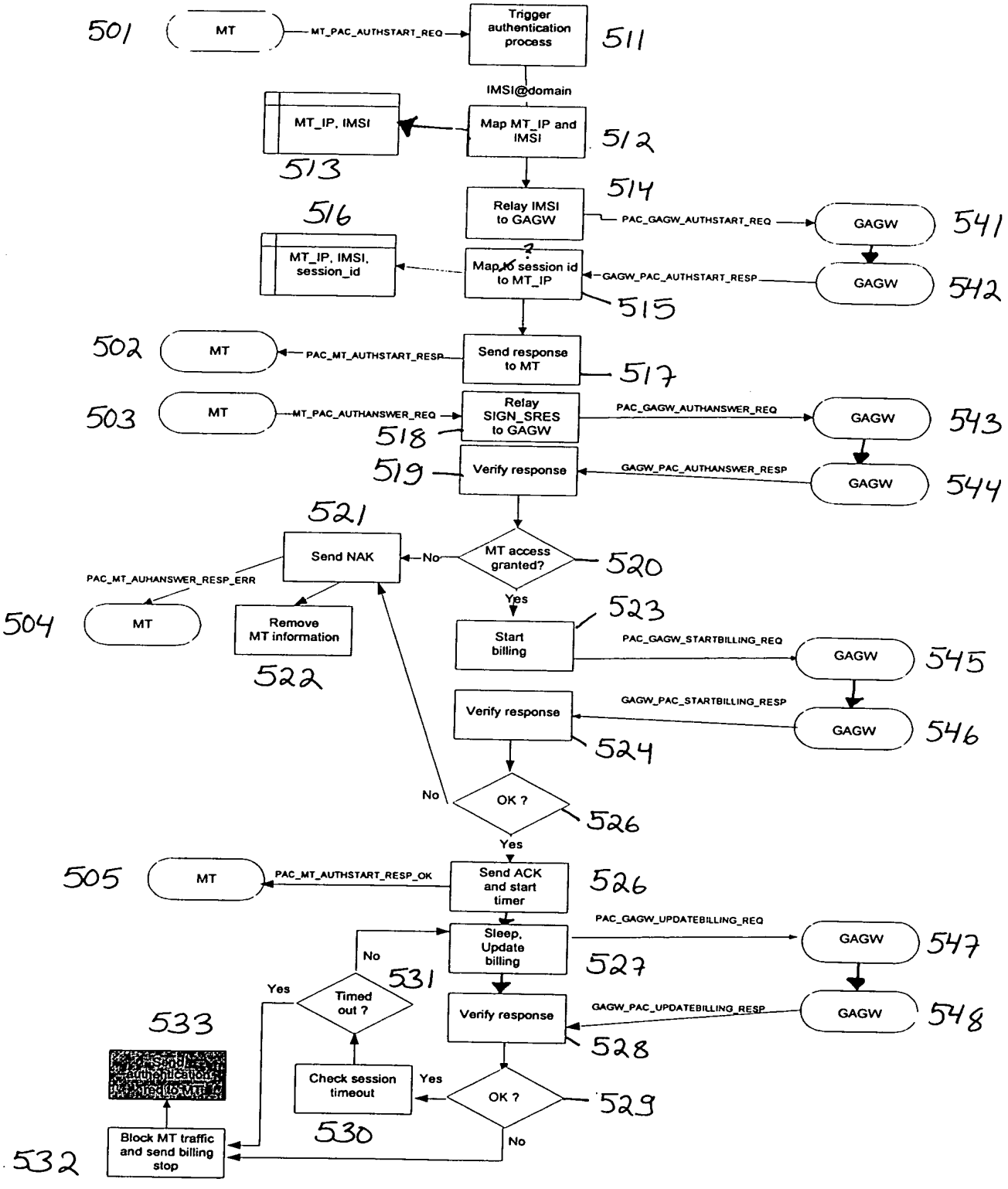
501
MT
MT_PAC_AUTHSTART_REQ
Trigger authentication process
511
IMSI@domain
MT_IP, IMSI
Map MT_IP and IMSI
512
513
514
Relay IMSI to GAGW
PAC_GAGW_AUTHSTART_REQ
GAGW
541
516
MT_IP, IMSI, session_id
Map to session id to MT_IP
GAGW_PAC_AUTHSTART_RESP
GAGW
542
515
502
MT
PAC_MT_AUTHSTART_RESP
Send response to MT
517
503
MT
MT_PAC_AUTHANSWER_REQ
Relay SIGN_SRES to GAGW
PAC_GAGW_AUTHANSWER_REQ
GAGW
543
518
519
Verify response
GAGW_PAC_AUTHANSWER_RESP
GAGW
544
521
Send NAK
No
MT access granted?
520
PAC_MT_AUHANSWER_RESP_ERR
504
MT
Remove MT information
522
Yes
523
Start billing
PAC_GAGW_STARTBILLING_REQ
GAGW
545
Verify response
GAGW_PAC_STARTBILLING_RESP
GAGW
546
524
No
OK ?
526
Yes
505
MT
PAC_MT_AUTHSTART_RESP_OK
Send ACK and start timer
526
PAC_GAGW_UPDATEBILLING_REQ
Sleep, Update billing
GAGW
547
527
No
531
Yes
Timed out ?
Verify response
GAGW_PAC_UPDATEBILLING_RESP
GAGW
548
533
528
Check session timeout
Yes
OK ?
529
530
No
532
Block MT traffic and send billing stop

Fig. 11

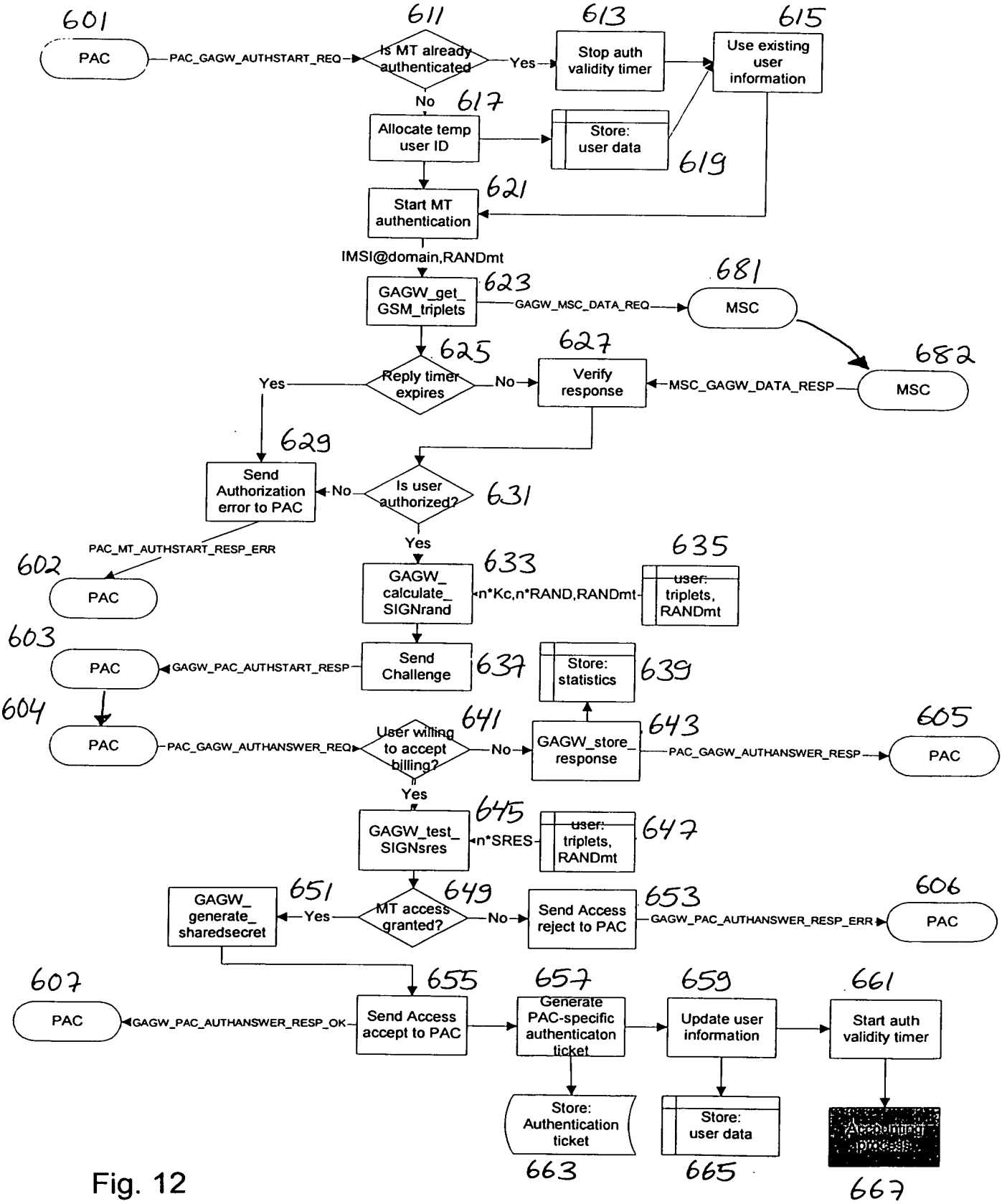
601
PAC
PAC_GAGW_AUTHSTART_REQ
611
Is MT already authenticated
Yes
613
Stop auth validity timer
615
Use existing user information
No
617
Allocate temp user ID
Store: user data
619
621
Start MT authentication
IMSI@domain,RANDmt
GAGW_get_ GSM_triplets
623
GAGW_MSC_DATA_REQ
681
MSC
682
MSC
627
Verify response
MSC_GAGW_DATA_RESP
625
Reply timer expires
Yes
No
629
Send Authorization error to PAC
No
Is user authorized?
631
Yes
PAC_MT_AUTHSTART_RESP_ERR
602
PAC
633
GAGW_ calculate_ SIGNrand
n*Kc,n*RAND,RANDmt
635
user: triplets, RANDmt
603
PAC
GAGW_PAC_AUTHSTART_RESP
Send Challenge
637
Store: statistics
639
604
PAC
PAC_GAGW_AUTHANSWER_REQ
User willing to accept billing?
641
No
GAGW_store_ response
643
PAC_GAGW_AUTHANSWER_RESP
605
PAC
Yes
GAGW_test_ SIGNsres
645
n*SRES
user: triplets, RANDmt
647
GAGW_ generate_ sharedsecret
651
Yes
MT access granted?
649
No
Send Access reject to PAC
653
GAGW_PAC_AUTHANSWER_RESP_ERR
606
PAC
607
PAC
GAGW_PAC_AUTHANSWER_RESP_OK
Send Access accept to PAC
655
Generate PAC-specific authenticaton ticket
657
Update user information
659
Start auth validity timer
661
Store: Authentication ticket
663
Store: user data
665
667

Fig. 12

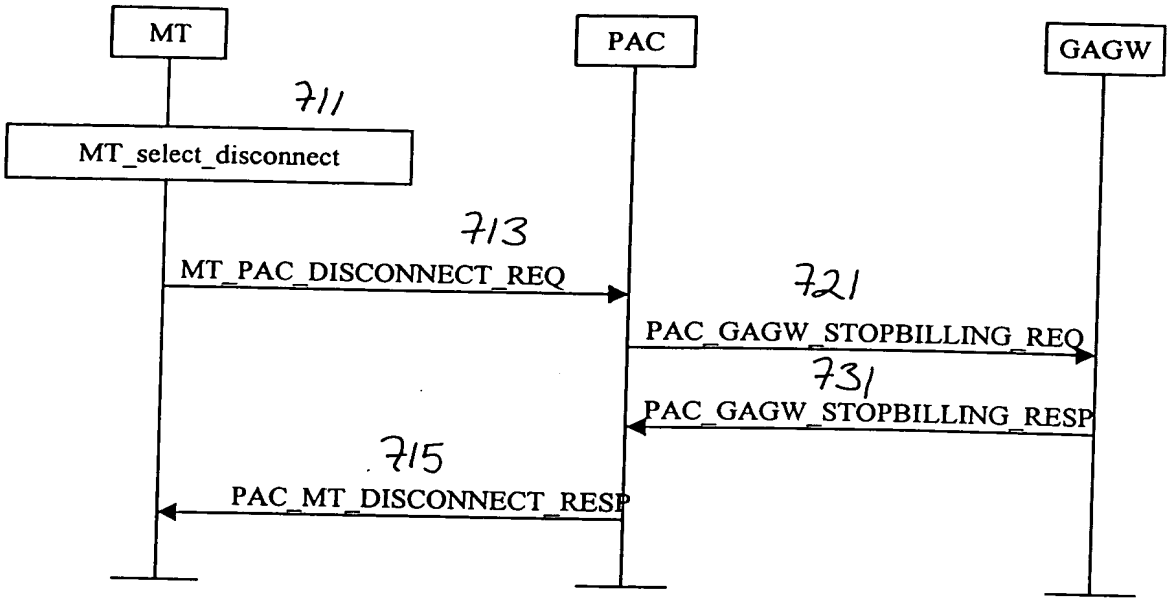
MT
PAC
GAGW
711
MT_select_disconnect
713
MT_PAC_DISCONNECT_REQ
721
PAC_GAGW_STOPBILLING_REQ
731
PAC_GAGW_STOPBILLING_RESP
715
PAC_MT_DISCONNECT_RESP

Fig. 13

#	MT	PAC	GAGW
(1)	HDR, SA, KE [, CERTREQ] =>		
(2)	<= HDR, SA, KE [, CERT_GAGW]		
(3)	HDR*, IDmt, Nmt =>		
(4)		IMSI, MN_RAND=>	
(5)		<= n*RAND, SIGNrand, MN_RAND, billingInfo	
(6)	<= HDR*, Npac, HASH(1), NOTIFY		
(7)	HDR*, HASH(2) =>		
(8)		SIGNsres, MN_RAND=>	
(9)		<= SIGNresult, MN_RAND, sessiontimeout, Kpac_MT	
(10)	<= HDR*, <SA_b>KpacMT, HASH(3)		

Figure 14

#	MT	PAC
(1)		<= HDR, SA
(2)	HDR, SA, KE [, CERTREQ] =>	
(3)		<= HDR, KE [, CERT_GAGW]

Fig. 15